Cymulate

Cymulate Solutions

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. The modular solution addresses a wide variety of business and technical use cases. With Cymulate, companies assess, optimize, and rationalize their security program with minimal resource investment. Security professionals leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to management and boards, and for compliance and regulatory programs.

Business Benefits

Measure Cybersecurity with the Same Diligence as Other Business Processes

All aspects of business operate with checks and balances to ensure that operations are working and delivering the expected results. Cybersecurity is no different and is expected to report on the efficacy of its operations in a timely and straightforward way. Cymulate safely provides efficacy validation of security controls with offensive attack simulations to test in-depth for detection, alerting, and defense. Additionally, businesses quickly gain insights into breach feasibility based on over 120,000 out-of-the-box simulations and the ability to create custom campaigns to test what companies are most concerned about.

Justify Budget & New/Existing Investments

Whether buying new security tools or justifying existing ones, Cymulate test simulations assess if tools are working as expected, if there are redundancies or gaps, and if changes in architecture could affect the company's risk score and profile. Cymulate is commonly used for investment decision-making, such as for new product comparisons or determining whether companies should renew existing infrastructure. The combination of technical and business reporting makes this a resource of choice for security teams and management.

Set & Track KPIs

Cymulate provides security leaders with a quantifiable measurement of risk to establish a baseline and track it over time. This measurement creates visibility of an organization's security posture for stakeholders, enabling data-driven decisions to rationalize investments and priorities. By establishing a clear baseline, security leaders measure and demonstrate success, as well as increase alignment with business and technical stakeholders by focusing on the same data-based analytics. Commonly used Cymulate KPIs include: mean time to detect (MTTD), mean time to respond (MTTR), incident response time, security control accuracy, and more.

Minimize Risk/Drift Detection & Control

Cymulate takes a proactive approach to minimizing risk exposure with continuous security validation. An organization's level of cybersecurity is as dynamic as its information network is and subject to fluctuations, much like market conditions and competitive pressures in other areas of business. Cymulate provides a framework for security teams to monitor risk levels so they can quickly remediate following events that cause security drift and increase exposure.

Mergers & Acquisitions (M&A)

Cymulate's security validation technology is applied on an M&A target infrastructure to map security gaps and provide a clear assessment of the cybersecurity risk associated with the potential acquisition. These assessments aid in due diligence, identification of issues to be addressed before and during the infrastructure merge, and strategic planning following the M&A regarding the merging of tools, platforms, and other applications.

Supply Chain Validation

With authorization, Cymulate is used to gauge the attack surface of a company's third-party organization to aid with vendor security compliance adherence. Depending on the access rights granted to a software supplier, this use case makes it easy to assess the damage an attacker could inflict. Additionally, when there is new intelligence on threats involving an organization's supplier or other third parties, Cymulate provides the ability to assess the impact on the organization and assists in planning defensive and remediation efforts.

Compliance & Assurance

Cymulate enables organizations to prepare for audits and other compliance operations. By creating, managing, and reviewing extensive simulations, organizations determine what remediation is required to bring environments into compliance prior to official certifications and other audit operations. Every test is documented, providing auditors with evidence of compliance with security testing mandates.

Risk-Informed Decision Making

Most organizations rely on data from security detections. The Cymulate platform provides offensive data-driven insights that proactively highlight high-risk security deficiencies and quantify risk. This provides organizations the ability to reduce risk by prioritizing vulnerabilities and finding misconfigurations that could be exploited by attackers. Additionally, executive reporting provides risk benchmarks and translates technical findings into a report that is consumable by business leaders.

Technical Use Cases

Cybersecurity professionals, regardless of industry, need visibility into the full spectrum of their organizations' exposure and breach feasibility. The three fundamental areas that should be continuously monitored are an expanding attack surface, potential attack paths, and the efficacy of security controls. The Cymulate Platform—including Attack Surface Management (ASM), Continuous Automated Red Teaming (CART), and Breach and Attack Simulation (BAS)—addresses these challenges and provides solutions for businesses of all sizes.

External Asset Discovery

External asset discovery provides organizations with automated reconnaissance to discover vulnerabilities and potential doorways into the organization, such as open ports and exposed cloud storage. Cymulate's reconnaissance module creates a full catalog of IT assets, their types, and which can be accessed from the internet.
External asset discovery also includes:

- Shadow IT discovery
- Vulnerability scanning
- First and third-party risk evaluation

Security Control Validation

Cymulate automates security control validation and enables continuous security control optimization. Applying a purple teaming approach, out-of-the-box assessments make it simple for all skill levels to know, control, and optimize the efficacy of security controls. The attacks are comprehensive and customizable, as well as safe to launch in the production environment.

Drift Control

Cymulate provides monitoring for security teams to assess risk levels so they can quickly find and remediate security drift. Findings include whether a solution is operating correctly and whether it is detecting and alerting accurately.

SIEM, SOC & IR Optimization

Through API–based integrations, simulated attacks are correlated with SIEM and SOAR findings. Analysts easily ascertain if the relevant events are being displayed by the SIEM and SOAR or if an alert was properly triggered. An organization's custom queries can be imported into the platform to validate their detection of malicious behaviors. Additionally, the platform provides Sigma rules for security analysts to implement. The platform's assessments are also commonly used by security teams to assess their incident response plans during tabletop exercises.

Immediate Threat Simulation

The Cymulate Immediate Threat Intelligence module is updated daily with new threat assessments. The platform safely deploys these simulations in a company's production environment to validate its defenses and if it is effectively protected against the latest threats found in the wild. Cymulate also provides actionable remediation guidance to close security gaps created by the new threat.

Vulnerability Prioritization

Cymulate's Vulnerability Prioritization Technology (VPT) integrates with common vulnerability scanners to inform security teams about the effectiveness of compensating controls protecting vulnerable machines and assets. VPT combines the results of Cymulate's simulated attacks with data from the organization's vulnerability scanner to accurately prioritize vulnerability remediation, patching, or reconfiguration of compensating security controls. Additionally, with these findings, Cymulate correlates the criticality of vulnerabilities with the value of assets for optimizing patching prioritization and reducing patching workloads.

Custom Attack Scenarios

Cymulate's Advanced Scenarios provides organizations with a customizable open attack framework to reduce time to remediation with a continuous feedback loop. Infosec and Purple Teams can create, store, modify, and execute both simple and sophisticated assessments using custom-built or out-of-the-box templates. Mitigation guidance following each assessment provides teams with easy-to-digest instructions for remediation.

Application & Cloud Security Validation

With Cymulate, security teams can discover and analyze security gaps and misconfigurations in their application and cloud infrastructure. For example, the platform provides organizations with an understanding of where a malicious actor is likely to begin when attempting to attack a cloud environment. Cloud-hosted security solutions can also be assessed to confirm that malicious activity is detected and blocked.

Red Team/Pen Test Automation

Cymulate provides Red Teams a platform to increase their operational efficiency and scale their adversarial activities in a production-safe environment. Assessments are easily customized, automated, and scheduled. Blue Teams that want to run offensive campaigns can also benefit from these capabilities with easy-to-use, out-of-the-box assessments.

Cymulate

Attack Path Mapping

Cymulate continuously validates the efficacy of network segmentation policies by mapping propagation tracks throughout the network and between segments, assessing opportunities for lateral movement. The platform continuously discovers discrepancies and provides remediation guidance, so security teams reduce risk by closing gaps and preventing security drift.

Privilege Policy & Identity and Access Management (IAM) Policy Validation

By running Cymulate's IAM assessments to test detection rules within a SIEM, organizations continuously validate that any administrative activity in these platforms generates alerts correctly. These simulations assess the detection of unauthorized and unauthenticated attempts to access sensitive data and abnormal behaviors that do not match roles and permissions.

Phishing Awareness Assessment

With Cymulate's Phishing Awareness module, organizations evaluate employee cybersecurity education programs by simulating phishing campaigns and identifying potential target opportunities. It can reduce the risk of data breaches, minimize malware-related downtime, and save money on incident response. Assessment results are shared with employees to maintain a high level of awareness.

Continuous Threat Exposure Management

Gartner has introduced a Continuous Threat Exposure Management (CTEM) program, which provides guidance and best practices for identifying, prioritizing, and addressing security risks in a continuous and systematic way. Cymulate aligns with CTEM's methodology by consolidating Attack Surface Management (ASM), Breach and Attack Simulation (BAS), and Continuous Automated Red Teaming (CART) into one platform to provide a comprehensive solution for security posture management. Cymulate is the partner of choice for companies interested in rolling out a CTEM program and minimizing cyber risk over time.

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