

Justify Budget & New/Existing Investments

Solution Brief



Challenges

The value of cyber programs is often difficult to quantify because there is a lack of standardization and widely accepted metrics for measuring the effectiveness of cyber programs. This makes it challenging to demonstrate the return on investment (ROI) of cyber initiatives and secure funding for cyber assets. The difficulty of showing ROI makes it harder for information security leaders to justify requests for budgets and resources.

Effectively quantifying risk exposure requires establishing a performance baseline and continuously measuring an organization's actual defense efficiency against cyberattacks.

Overview

Whether buying new security tools or justifying existing ones, Cymulate test simulations continuously 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.

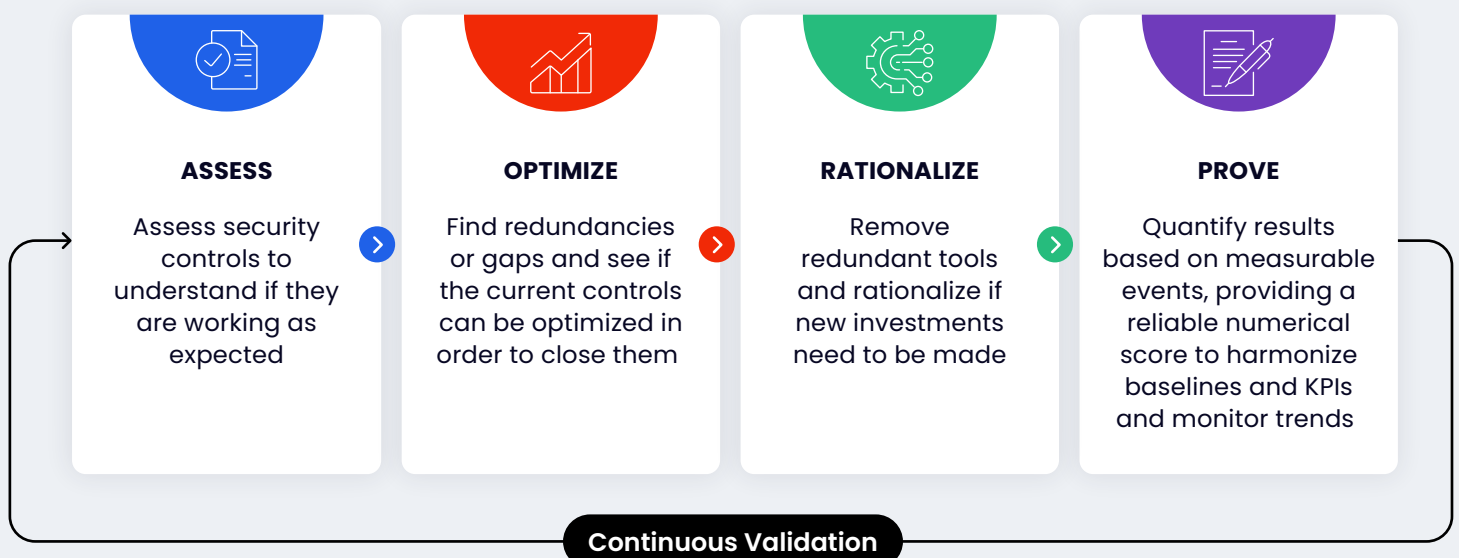
Cymulate's algorithm calculates security scores using industry-recognized standards such as the NIST Risk Management Framework, CSVSS v3.0 Calculator, and Microsoft's DREAD. The results are quantified based on measurable events, providing a reliable numerical score that can be used as a base to harmonize baselines and KPIs and monitor trends.

Cymulate is commonly used for investment decision-making, such as for product comparisons, headcount quandary and even due diligence before M&A activities.

Benefits

- **Attack-based analytics** assess security controls for block and detection rates, determining if the current controls are effective or should be replaced.
- **Technical and executive reports** provide a comprehensive overview of an organization's security posture and generate insights into where security is strong, where there are redundant tools, and where more resources are needed.
- **Simulated attacks validate new vendor's claims** during a POC in an organization's actual environment and help determine which tool works best.

How the Solution Addresses the Problem Statement Above



Main Features



Attack-based analytics assess security controls for block and detection rates, determining if the current controls are effective or should be replaced.



Technical and executive reports provide a comprehensive overview of an organization's security posture and generate insights into where security is strong, where there are redundant tools, and where more resources are needed.



Simulated attacks validate new vendor's claims during a POC in an organization's actual environment and help determine which tool works best.

Case Studies and Customer Success Stories



I showed our board of directors the comprehensive visibility that Cymulate provides, and they told me that we needed it before I even had the budget to purchase it.

Cymulate provides us with the insights to close gaps and optimize the controls we already have in our security stack—we don't need to waste time or money looking for new tools to improve our security.

Liad Pichon, Director of Cybersecurity, BlueSnap



With Cymulate, the Persistent CISO can easily communicate to the executive board where he needs to focus his manpower and budget. He can consistently show a direct correlation between the investment in his security program and the reduction of overall risk.

Excerpt from the case study **Persistent Systems Gains Visibility & Control of its Security Posture.**

[Read more](#)



The assessments provided Craig Bradley, Senior VP of IT, and his team the visibility they required and the guidance to improve the performance of the technologies they had in place. It also allowed Craig to justify budget requirements, allocate resources effectively, and make targeted procurements.

Excerpt from the case study **YMCA Greater Toronto (YMCAGTA) Maximizes Value from their Existing Security Architecture**

[Read more](#)

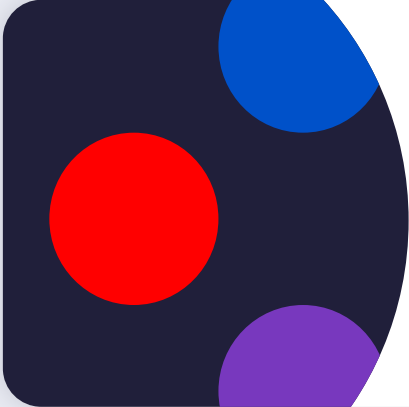


Cymulate allows us to evaluate the efficacy of a specific tool and ensure the product works as advertised. Simulations also help us determine the proper configuration so we can make a data-based decision about a tool's performance. Additionally, based on the data and analytics from Cymulate's assessments, I can build a transparent business case when I ask the CEO for budget.

Itzik Menashe, VP Global IT & Information Security, Telit
Excerpt from the case study **Telit Validates Security Controls with Cymulate.**

[Read more](#)

Additional Resources





Cymulate Business Justification

[Read more](#)

Backed by the Industry

Awards and Accolades



About Cymulate

The Cymulate Security Posture Validation Platform provides security professionals with the ability to continuously challenge, validate, and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy, and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.

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

[Start Your Free Trial](#)

info@cymulate.com | www.cymulate.com