

Set and Track KPIs

Solution Brief

Challenges

The lack of standardization in cybersecurity metrics and benchmarks impedes the establishment of industry-wide, normalized baselines for KPIs. At an organizational level, baselines relying on adhering to standards such as NIST or CIS controls do not provide a contextually accurate security posture evaluation and detect and respond technologies only measure what they can detect, leaving significant blind spots in the assessment of the true level of protection against known and emerging threats.

In addition, the constantly evolving nature of cybersecurity requires KPIs to be continuously updated and adjusted to remain relevant, and differing definitions of a secure environment and varying risk tolerance levels further complicate aligning cyber KPIs with business strategy.

Overview

Cymulate provides standardized metrics and benchmarks that enable the establishment of a common baseline for KPIs. The Cymulate continuous and automated security validation platform provides ongoing testing of an organization's cybersecurity posture against real-life cyber threats. Its risk-scoring feature provides a validated, quantified, and asset-mapped evaluation of an organization's threat exposure.

The Cymulate attack-based risk analysis feature identifies redundant and inadequately configured solutions, providing crucial information for rationalizing, optimizing, and streamlining the cybersecurity tool stack.

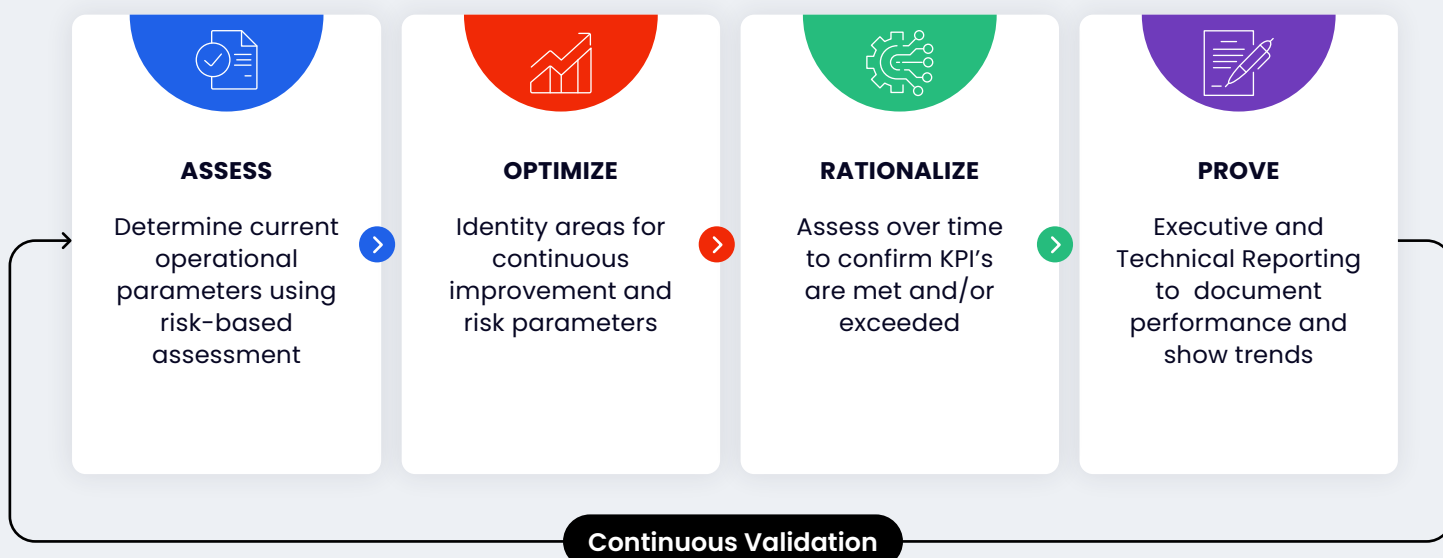
With a clear view of the organization's exposure landscape and quantified risk scores, business stakeholders can make informed decisions about balancing security and business priorities and define environment-specific risk appetite.

With clearly defined baselines, security leaders can measure and demonstrate success and increase alignment with business and technical stakeholders by focusing on the same data-based analytics.

Benefits

- > 360° security posture visibility
- > Prioritized workloads
- > Focused metrics for data-based decisions
- > Security drift detection and prevention
- > Increased collaboration
- > Improved communication with leadership
- > Streamlined patching process based on risks
- > Mitigation traceability

Define and Track KPIs with Cymulate



Main Features



Attack-based data evaluation assesses exposed assets and validates the efficacy of security controls.



Pre-loaded drift detection and vulnerability management dashboards identify potential vulnerabilities and assess mitigation efforts' efficacy.



Customizable dashboards and reports equip CISOs to select relevant data and present it in an easily understandable format to stakeholders.



Attack-based vulnerability management focuses remediation efforts on the most impactful mitigation efforts, optimizing resource efficiency.

Case Studies and Customer Success Stories

Euronext

Leading Pan-European trading marketplace with 1,300 domestic and foreign companies listed for trading and a combined Euro 3.5 trillion market capitalization.

- **Challenge**
Euronext sought a more efficient and cost-effective way to continuously test its security posture
- **Solution**
By deploying Cymulate, Euronext can quickly run simulations of the very latest cyberattacks, repeatedly and frequently.
- **Benefits**
The team can easily determine the impact of new technology, security controls, and configuration changes on its security stack while proving the value of business decisions with transparency.

[Read more](#)

Singular Bank

Singular Bank is an independent Spanish bank that helps its clients define and achieve their financial objectives based on an advanced technology platform.

- **Challenge**
Singular Bank wanted visibility into its security controls to validate their effectiveness and decrease the organization's level of risk.
- **Solution**
By implementing Cymulate, Singular Bank validates its security posture on an automated and continuous basis, quickly obtaining reliable results and objective data to optimize its security posture.
- **Benefits**
With less effort and at a lower cost, Singular Bank effectively validates its security posture and uses Cymulate's analytics to measure and communicate success to the management.

[Read more](#)

Additional Resources



Cymulate Business Justification

[Read more](#)

Backed by the Industry

Awards and Accolades



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 gain evidence for compliance and regulatory purposes.

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

[Start Your Demo](#)

info@cymulate.com | www.cymulate.com