

CASE STUDY

IT Services & Consulting Organization Improves Security Effectiveness and Reduces Risk with Cymulate

Limited Visibility into Security Effectiveness and Emerging Threats

Protecting sensitive data and maintaining regulatory compliance are critical priorities for this IT services and consulting organization, driving its security team to continuously assess and strengthen its defenses.

As an ISO-certified company, quarterly vulnerability assessments and penetration tests via third-party organizations met the minimum requirements for audits and various global industry regulations, but the security team recognized that compliance does not always equal better, stronger security.

To go beyond compliance, the security team faced the following security challenges:

- **Continuously validating its security performance.** Despite quarterly penetration tests, the security team did not have a complete picture of its security posture. These penetration tests were point-in-time assessments and evaluated security posture solely based on penetration paths and vulnerabilities without considering security controls.
- **Enforcing global IT security policies.** The company has over 50 offices in 18 countries, and many employees work from home, making security policy validation a daunting task. The security team created multiple access management and network segmentation policies to keep the company safe. However, without continuous validation, misconfigurations or security drift can cause gaps that can be exploited if not found in time.
- **Staying up to date on emerging threats.** With new threats emerging daily, the security team was responsible for reporting to management on whether the company would be protected from the latest threat—before an attack took place—and planning accordingly. However, the team had limited real-time access to threat intelligence, which left them vulnerable.

Understanding these shortcomings, the team researched platforms for continuous validation, focusing specifically on automated tools that reduce human effort and consistently provide high-impact assessments for accurate evaluation.

The Cymulate Solution

The CISO explained that when assessing different security validation tools, it was important that the solution provide both control and threat validation. The CISO selected Cymulate over other platforms because it covered them both extensively, while also enabling the team to prioritize exploitable exposures, streamline remediation efforts and foster collaboration between offensive and defensive teams.

Overview

Industry	IT Services & Consulting
HQ	APAC
Company Size	22K+ employees



With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk.

— CISO

Use Case

- Threat Validation
- Control Validation and Optimization
- Exposure Prioritization and Mitigation

Results

- Continuous security validation
- 70% reduction in critical vulnerabilities detected in a pen test
- Reduced from 1.5 days to 1-3 hours to analyze data

Security control validation and optimization

“With Cymulate, the SecOps team ensures that our security policies and controls are consistent throughout the organization and that there are no gaps for attackers to breach our network. Easy-to-digest mitigation guidance following each assessment, combined with the Mitigation Hub’s centralized remediation workflows and tracking, allows the SecOps team to prioritize, manage and accelerate remediation efforts.”

– CISO

Continuously updated threat intelligence

“Cymulate Research Labs updates the platform daily with new prepackaged threat assessments so our security team can immediately test their security controls against the latest threats, with no added effort.”

– CISO

Vulnerability prioritization

“Cymulate provides a comprehensive overview of our IT environment, adding context to vulnerabilities and correlating their criticality with the value of assets. We’ve been able to automate our vulnerability management process and quickly prioritize remediation activities with minimal effort.”

– CISO

Red and purple teaming

“The red team uses Cymulate Threat Studio to automate and scale its adversarial assessments, continuously emulating real-world attacks and uncovering security gaps. Findings are automatically collected in the Mitigation Hub, enabling the security team to quickly prioritize and remediate before an attacker can exploit them.”

– CISO

Benefits

- **Monitored security drift** — Cymulate enables the team to keep risk low and automatically monitors for security drift. If an increase in the risk score is detected, the team is notified immediately so it can remediate and fine-tune its controls.
- **Hardened security posture** — The team’s most recent third-party penetration test and vulnerability assessment found 70% fewer critical vulnerabilities than usual. Consequently, the organization plans to reduce the cost of future vulnerability assessments by pricing them according to the number of critical vulnerabilities found rather than the number of vulnerabilities they scan for.
- **Data-based analytics** — Before implementing Cymulate, it took about a day and a half to manually collect data, analyze the results and make meaningful decisions. With Cymulate Vero AI creating customized dashboards, the team now spends just 1-3 hours evaluating results and making faster, more informed decisions.
- **Improved communication** — With Cymulate, the CISO can easily communicate with the executive board about where he needs to focus his manpower and budget. He consistently shows a direct correlation between the investment in his security program and overall risk reduction.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.