cymulate

CASE STUDY

IT Services & Consulting Organization Hardens Security Posture with Cymulate Automated Security Validation

Challenge

The security team at this IT services and consulting organization is responsible for protecting the company's and its end-customers' data. As an ISO-certified company, it conducts quarterly vulnerability assessments and penetration tests via third-party organizations to stay up to date on audits and comply with various global industry regulations.

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 being introduced daily, the security team was responsible for reporting to management if the company would be protected from the latest threat — before an attack took place — and planning accordingly. However, the team had limited access to threat intelligence in real time, 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 organization's CISO explained that when assessing different security validation tools, the organization considered three top use cases and selected Cymulate over the other platforms because it covered them all extensively. Those use cases were: security control validation, IT security policy enforcement and immediate threat intelligence.

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

Solution

- Breach and attack simulation (BAS)
- BAS advanced scenarios
- Continuous automated red teaming

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

The CISO elaborated how his team uses Cymulate for the top three use cases:

Security control validation and threat exposure assessment

"With Cymulate, the SecOps team ensures that our security policies are consistent throughout the organization and that there are no gaps for attackers to breach our network and gain an initial foothold. The team also continuously validates our security controls. Easy-to-digest mitigation guidance following each assessment allows the SecOps team to focus on its remediation efforts."

IT security policy enforcement

"With Cymulate BAS Advanced Scenarios, the team customizes complex scenarios from pre-built resources and custom binaries and executions without limits or restrictions. The team runs continuous assessments to validate network segmentation and explore if an attacker can move laterally within the network after gaining an initial foothold."

Immediate threat intelligence

"The Cymulate Threat Research Group 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."

In addition to these use cases, the CISO explained that his team also uses Cymulate for:

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."

Red team automation and customization

"The red team uses Cymulate BAS Advanced Scenarios to automate its assessments and scale its adversarial activities with proactive threat hunting and health checks. Any gaps found during these assessments are automatically documented in a mitigation report so they can be remediated immediately before an attacker can exploit them."

Benefits

- **Monitored security drift** — Cymulate enables the team to keep its 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 and analyze the results before making meaningful decisions. Now, the team only needs to invest about 1-3 hours to evaluate the data from Cymulate's dashboards to make data-based decisions efficiently.
- **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 exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.