cymulate

Betting on Cybersecurity: How a Gambling Innovator Plays It Safe with Cymulate

CASE STUDY

When Manual Testing Isn't Enough

In the high-stakes world of online gambling, the odds aren't just for players; they're also for cybercriminals looking to cash in. This organization supplies gambling platforms and software to online casinos, bingo operators and lotteries in a highly regulated industry. Because cyber attacks on the gambling industry have increased in the past few years, this company's security team must assure its clients that their information is secure. The team also needs to protect its internal staff, operations and business continuity.

The security team understood that to stay ahead of cyber attacks, it needed to proactively identify gaps in its security and mitigate them before an attacker could take advantage. In addition to running vulnerability assessments, the security team outsourced manual penetration tests annually as well as occasionally if there was a major change in the organization's infrastructure. However, these penetration tests were:

- Expensive and infrequent; they only provided a point-in-time snapshot of the company's security posture and didn't consider continuously emerging threats.
- Focused on finding security gaps but did not prioritize or guide the remediation process.
- Unable to immediately confirm if remediation efforts would prevent a future breach.

The organization's Head of Information Security and Business Continuity wanted an alternative solution to penetration tests that would provide continuous security validation and visibility of its exploitable security gaps. This would also allow the team to evaluate which exposures to prioritize based on their potential impact on the organization's most critical assets.

The Cymulate Solution

As a previously satisfied Cymulate user, the Head of Information Security and Business Continuity knew that Cymulate was the answer to his team's need for continuous validation. He explained, **"As a security leader with a lot of technical expertise, it's easy to think the business is protected because you have the right controls in place. Cymulate brings you back to reality to show where you have gaps and the steps you need to take to strengthen your defenses."**

The Head of Information Security and Business Continuity elaborated that his team uses Cymulate to optimize defenses, stay ahead of emerging threats, validate compliance and focus remediation on the highest-risk vulnerabilities.

Overview

Industry	Software development
HQ	UK
Company Size	201-500 employees

> "Cymulate is a proactive security tool that allows us to validate threats before they become a major risk to the organization."
>
> – Head of Information Security and Business Continuity

Solution

- Breach and attack simulation
- Phishing awareness

Results

- Validate security continuously
- Assess against new threats as they emerge
- Prioritize exploitable vulnerabilities

Continuously validate and optimize its security controls

"Before Cymulate, I thought our anti-malware protection was performing properly because we invested time and effort in configuring it. After running the simulated assessments, Cymulate highlighted problems with the anti-malware control's configuration and that its updates were not getting rolled out quickly enough to our endpoints. Cymulate identified the gaps and guided us on how to fix them."

Ensure protection against one-day exploits

"Cymulate immediate threat assessments are a great way to test controls against one-day exploits within our business and mitigate weaknesses before they become a problem."

Prioritize vulnerabilities

"Vulnerability assessments give us a long list of vulnerabilities, and if we tried to remediate them one by one, we wouldn't get to them all. Cymulate security validation allows us to understand which of those vulnerabilities can actually be exploited, and those are the ones we know we need to prioritize and fix."

Evaluate phishing awareness

"Each month, my team builds a Cymulate phishing campaign. We track the metrics to understand how many people clicked on a link in the phishing email and gave their usernames or passwords. Now, we have a full picture of which employees are vulnerable, and we can educate them so they don't fall victim to a phishing email."

Prove compliance

"We get audited about every other week, and usually, the auditors want to understand the controls we have in place and how we operate those controls to protect the business. With Cymulate, we easily demonstrate how our controls are performing and that by continuously assessing them, we can fix any gaps as soon as we are alerted about them."

Benefits

- **Visibility of security gaps** — Cymulate's continuous assessments consider the dynamic threat landscape and provide the team with immediate visibility of its security gaps.
- **Validate operational resilience** — The security team can run tabletop exercises with Cymulate to practice incident response and ensure operational resilience in case of attack.
- **Strong customer support** — The security team views Cymulate as a partner in its cybersecurity journey, and they hold monthly meetings to collaborate and ensure goals are aligned and achieved.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.