cymulate

CASE STUDY

Civil Engineering Organization Goes Beyond Security Control Validation with Cymulate

Challenge

This engineering, architecture, and construction services company has 160 offices on five continents, close to 15,000 employees and clients in multiple industries, making it a complex organization to keep secure. The SecOps team includes seven internal team members responsible for incident response, vulnerability management and threat intelligence, and it employs an external MSSP for 24/7 monitoring.

The team conducted third-party annual penetration tests for compliance reasons, but these assessments were point-in-time, limited in scope and did not provide complete visibility. Additionally, the team would remediate following a penetration test, but there was no way for the team to know if the efforts successfully reduced risk.

The team had been using Cymulate to continuously validate its security controls and assess their effectiveness, especially following remediation. However, when a new SOC manager joined the organization, he noticed his team could use the platform in more cases. He reflected, **"I immediately identified opportunities for Cymulate to be used to do more and was surprised that the team was only using it for automated security control validation. There was so much more value to be realized from the platform's comprehensive capabilities."**

The Cymulate Solution

The SOC manager worked with his Cymulate customer success representative to optimize the use of the platform. The SOC manager explained that today, in addition to continuous security validation, his team uses Cymulate to:

Test against emergent threats

"We automate the Cymulate immediate threats assessments to validate our controls for any new threat found in the wild. Because the Cymulate Threat Research team adds new assessments as the threats emerge and the platform runs them automatically, it significantly reduces my team's manual efforts."

Automate IOC mitigation

"Before Cymulate, adding IOCs to our controls would have been a manual task for an analyst to do weekly. With the Cymulate IOC (indicators of compromise) mitigation capability, the platform automatically uploads critical IOC data to our web gateway and EDR. We have seen a direct connection between the newly added IOCs and our controls successfully detecting and preventing emergent threats."

Overview

Industry	Civil Engineering
HQ	Australia
Company Size	15,000 employees

> Cymulate is not only for security control validation; it also provides extensive intelligence on threats and vulnerabilities and gives you a comprehensive picture of your organization's cyber resilience — all in an automated fashion to increase team efficiency and accuracy.
> — SOC Manager

Solution

- Breach and attack simulation
- Continuous automated red teaming

Results

- Increased team efficiency
- Prove the value of cyber investments
- Visibility of cyber resilience

Prove cyber resilience

“We use Cymulate reporting to capture and report how our controls are blocking and preventing attacks based on the simulated assessments. We use data from Cymulate to support our cyber strategy.”

Prioritize vulnerabilities

“Before Cymulate, managing our complex vulnerabilities was challenging, especially communicating the urgency of remediating a specific vulnerability. We integrated our vulnerability management tool with Cymulate to highlight to the team which vulnerabilities need prioritization because they are exploitable in our environment.”

Validate remediation

“A few months ago, we conducted a third-party penetration test, which resulted in findings we needed to remediate. Following remediation, we ran a few Cymulate assessments and were able to validate that our efforts were successful immediately. Before Cymulate, we would have had to assume that our controls were tuned correctly — now we can independently validate with minimal effort and resources.”

Benefits

- **Valuable customer support —** The Cymulate customer success representative enables the security team to utilize the platform for more than continuous security validation, providing support at every step.
- **Proof of investment —** It isn't easy to measure the value of something that hasn't occurred, like a cyberattack. However, Cymulate shows the organization's stakeholders a direct connection between how a potential attack could have happened and the security team's successful prevention efforts.
- **Increased efficiency —** The platform's automation enables the team to improve its testing and remediation efforts. Because of the threat intelligence that Cymulate provides, the team can perform more tasks with better precision.

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.