cymulate

CASE STUDY

Utility Organization Validates Protection Against Emerging Threats with Cymulate

Challenge

This utility organization plans, manages, and develops its country's energy, making it susceptible to cyberattacks. Any downtime the organization might experience because of an attack would be detrimental to the country and its citizens.

The security engineering team manages the organization's security tools across three different systems, each with unique, complex IT requirements. The team's main challenges included:

- **Testing against emerging threats and APT attacks**
  Various threat feeds alerted the team to new threats, but the information overload made it challenging to understand which threats applied to the organization. Overall, the team still needed to investigate the threats and then build the resources and test cases to assess them.
- **Managing its external attack surface**
  The team would outsource third-party penetration tests against some of its core externally facing assets, but this did not ensure that all its internet-facing assets were secure.
- **Continuously testing its security controls**
  The organization conducted annual third-party penetration tests, but they were point-in-time assessments. The security team wanted continuous visibility of its security controls to ensure they kept up with the evolving threat landscape.

The Cymulate Solution

The security team decided to purchase Cymulate because it provided security control and threat validation, as well as attack surface management.

> Cymulate is the best-in-class for automated security validation. It offers the most breadth and depth of attack simulations, provides assessments against emerging threats and enables us to manage our attack surface.
> — SOC Manager

Overview

Industry	Utilities
HQ	EMEA
Company Size	201-500 employees

Solution

- Attack surface management
- Breach and attack simulation
- Continuous automated red teaming

Results

- Validated protection against emerging threats
- Increased SecOps efficiency
- Improved visibility of security posture

The organization's SOC Manager explains that the team uses Cymulate to:

Test against emerging threats and APT attacks

"The Cymulate immediate threats capability allows us to automatically test against new threats within about 24 hours of when the threat is first discovered. We no longer need to track our threat feeds and figure out which threat might be the riskiest to our organization. If a simulated threat does get through our defenses, our efforts can be focused on remediation."

Manage external assets

"Cymulate Attack Surface Management enables us to automatically identify our internet-facing assets and understand if there are any potential entry points or vulnerabilities within our external infrastructure. This allows us to manage our external attack surface effectively."

Continuously validate security controls

"We've completely integrated the Cymulate platform into our SecOps processes. Once the scheduled assessments automatically test our controls, we review the results. The team has procedures to quickly implement remediation guidance and optimize our security."

Provide evidence for regulatory compliance

"With Cymulate, proving we are following regulations takes less effort. We produce a report from the platform to show our security posture score, delivering evidence that we have full visibility and control of our attack surface, are continuously testing and improving our security posture, and staying ahead of emerging threats."

Benefits

- **Increased efficiency** — Cymulate enables the security team to automatically and continuously test its security independently. Once the team receives the assessment results, it can focus on remediation and optimizing its controls. Cymulate automated reporting allows the team to concentrate on other high-priority tasks.
- **Depth & breadth of testing** — Cymulate includes an extensive library of threat intelligence-led risk assessments. Additionally, automation enables the security team to scale its testing across the IT environment with detail into different layers of each control.
- **Prioritization** — Following a Cymulate assessment, the security team better understands its control gaps and prioritizes remediation for the areas most at risk of exploitation.
- **Comprehensive visibility** — Cymulate reporting and metrics provide the CISO visibility into the security team's activities. This allows the CISO to track the team's progress and ensure continued improvement.