Cymulate

Hedge Fund Optimizes Testing Against Emerging Threats with Cymulate

Organization

A global hedge fund with a few hundred employees has offices in the US, Hong Kong, and London. Its small security team of 5 is led by a CSO who is responsible for all cyber and physical security for the organization. The IT team takes a generalist approach to their security and protects against infrastructure attacks, ransomware, malware, phishing, and emerging threats in the financial space.

Challenges

The hedge fund faced three main challenges, all stemming from their lack of offensive security automation:

01 Inability to continuously validate security posture
With the constantly changing threat landscape and increased risk caused by undetected security drift, the hedge fund realized the importance of continuously testing their security controls to improve their security posture. However, the team did not have any automation in place, and manually validating controls was labor-intensive and time-consuming.

02 Difficulty testing immediate threats
When an emerging threat was published, the hedge fund would manually research the new threat and develop a simulated attack to test in their environment, which created multiple problems:

New threats were being introduced too frequently for the team to keep up.

- The longer it took to research each threat, the less they could focus on other tasks.
- If they wanted to use code from another source to save time, they weren't sure if they could trust that source to accurately duplicate the threat actors or run it safely in production.
- Even with access to reliable exploit code to run a simulated production-safe attack, cybercriminals' agility in pivoting with additional tools and new methods made that code rapidly obsolete.

Keeping up with threat actors' different methods, tactics, processes, and tools was overwhelming the security team's capacity.

03 Inefficient security operations
The hedge funds' CSO felt that manually testing security controls was a resource-intensive effort that not only included creating the tests, but also required cloning the environment to run the tests. Additionally, analyzing the tests' results was a complex and time consuming manual task followed by the necessity to manually run mitigation validation tests.

Challenge
Continuously validating the hedge fund's security controls and testing them against emerging threats was too difficult and time-consuming to accomplish manually with a small security team.

Solution
Cymulate provides an easy-to-use automation platform that helps validate security controls, test immediate threats, and scale adversarial skills to increase team efficiency.

Benefits
With Cymulate, the small security team can perform more tests, focus their remediation efforts, and continuously validate its security posture.

Solution

The CSO decided that Cymulate was the best tool for the hedge fund's security needs because it maximizes the efforts of its small security team and enables them to customize and execute adversarial assessments, without an in-house red team. The hedge fund uses Cymulate to:

- **Continuously validate security controls**
  The hedge fund can efficiently assess its security posture and draw a baseline to monitor how it trend over time. The team receives continuous evaluation of their security controls' efficacy and can easily plan remediation based on easy-to-digest recommendations. Once the security controls are reconfigured, automated security validation tests evaluate the impact on risk levels.

- **Customize and automate its own assessments**
  In addition to the provided out-of-the-box attacks, the team utilizes the Advanced Scenarios module to create, store, modify, and execute customized attacks for an added layer of protection. This feature enables the hedge fund's small security team to maximize its capabilities through continuous feedback by scaling adversarial skills and practicing Purple Teaming even without an in-house red team. This increases resilience both against emerging threats and against vertical and lateral progression

- **Test emerging and immediate threats**
  Once a new threat is discovered in the wild, Cymulate's research lab immediately develops a simulated attack that mimics all the exploit's steps, enabling the hedge fund to swiftly test its controls' efficacy against it. As the CISO explained, "We can send the simulated attack directly to our production environment and test it right away—no extra set up and no need to find a trusting source for a POC." He adds, "It allows us to turn it around in about half the time it would take us to do it all manually." In addition, tightened controls provide increased resiliency against zero-day attacks.

- **Evaluate current and new tools**
  The hedge fund's CSO can easily evaluate if a security gap is caused by a misconfigured control of a detection tool or a missing detection capability requiring additional tooling. He can also evaluate those new tools and examine how they perform in his environment against known threats, tactics, and techniques.

Benefits

The easy-to-use framework and production-safe testing enables effortlessly setting up simulated attacks in the hedge fund's own environment, combining out-of-the-box assessments and customized attacks as needed. The platform's automation facilitates increased testing frequency which provides continuous visibility of the hedge fund's security posture and risk levels.
In addition, the actionable remediation recommendations following an assessment accelerate mitigation.
The platform also operationalizes the MITRE ATT&CK framework to enable continuous assessment against real-world attack scenarios.

> *“With Cymulate, I can validate controls against emerging threats faster than I could before.”*
>
> *CSO, Global Hedge Fund*

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data.
Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Triel