CASE STUDY: FINANCIAL INDUSTRY

Hedge Fund

Executive Summary

This leading hedge fund has billions in assets under management and over 1,000 employees located in offices around the world. This hedge fund offers a full range of fixed income and equity strategies designed to target higher expected returns. Its portfolios are complex, developed with proprietary techniques and managed carefully with proprietary risk management techniques.

Over the past few years of increasing cyber threat activity, it was deemed critically important by this hedge fund that it becomes better equipped to accurately and objectively assess the performance of its security controls, personnel, and related processes. It felt that a breach and attack simulation (BAS) system operationalizing MITRE ATT&CK™ would best enable it to reach these goals. After considerable review, this leading hedge fund chose AttackIQ as the breach and attack simulation platform to support its efforts and began deployment in 2019.

> "MITRE ATT&CK gave us the ideal framework to meet our target use cases with AttackIQ's breach and attack simulation platform. It also made it easier to objectively manage accountability between the security operations, information technology, and our internal networking group. MITRE ATT&CK gave us a common language to use for precise communication amongst all of our cyber defender stakeholders and clear and measurable data that we can all use. It was also highly important to us that we could continually validate the performance of our production system security controls in real time - this was a critical part of our decision to acquire AttackIQ's platform."
>
> — Hedge Fund Cyber Defense Team

Over the past six months alone, the BAS platform has identified several new gap areas requiring remediation. The hedge fund teams have moved rapidly to close these gaps and reduce attendant risk. Given the recent success, this hedge fund has moved decisively to further deploy AttackIQ enterprise-wide, as it has validated the benefits of the platform and considers it an important and key component of its cyber defense strategy.

The Challenge

This hedge fund does business in a highly competitive industry. Its cyber defense team was recently expanded to include a new chief information security officer (CISO) and highly experienced team personnel, and it has been investing in new security controls continuously. Management understands the threats faced by its industry and has stepped up to provide the necessary support for an expanded cyber defense strategy.

It was important to the cyber defense team that the breach and attack simulation platform would support its requirements for expanded visibility into its security controls. The team wanted to be immediately aware of any gaps in its defenses. The team also wanted to be able to assess its network defenses against the known threats that it is most likely to face based upon

industry knowledge and threat intelligence. In addition, the cyber defense team wanted to be able to simulate how those threats might target and penetrate its networks and assets.

Most important, this hedge fund wanted to know that, while network penetration was possible, it had the critical defense components in place and correctly configured to identify and stop the attack path before malicious actors could exfiltrate confidential personal data or financial assets.

The Situation

This hedge fund must protect thousands of users across a mix of on-premise, cloud, and SD-WAN-connected remote facilities. As with many other growing companies going through a digital transformation, this has required an increasingly complex set of differing security stacks for adequate defense and threat mitigation. The volume of ongoing attacks in the financial industry presents an ever-increasing risk to the hedge fund's business operations and assets.

The hedge fund must also meet strict compliance requirements that necessitate red team penetration testing. The hedge fund's cyber defense team wants to increase red team effectiveness and capabilities, add precision to the blue team's remediation, and enable thorough validation by its purple team.

The Solution

AttackIQ's BAS technology allowed this leading hedge fund to rapidly automate and operationalize MITRE ATT&CK. The hedge fund's red team can now emulate the full attack and expanded Kill Chain against enterprise infrastructure using AttackIQ. This enables it to find the performance gaps in its systems, prioritize and remediate these gaps, and support continued red team testing to validate that these gaps remain closed.

Its cyber defense team was able to implement the AttackIQ BAS platform rapidly and effectively. It completed deployment for a few thousand users before rapidly expanding its efforts to complete enterprise-wide deployment.

Outcomes

This leading hedge fund used MITRE ATT&CK and AttackIQ's BAS platform to initially address three key use cases. The first important use case was to provide support for vendor security control evaluations. This hedge fund was able to compare and contrast endpoint detection and remediation (EDR) vendor alternatives and to determine precisely, as configured, which would provide the coverage best for its environment.

The second use case was that BAS automation supported the hedge fund team's requirements for continuous security validation (CSV). CSV enabled it to achieve what is referred to as "knowledge compounding." The BAS system effectively compounds the hedge fund's knowledge growth by validating all of its current controls as configured and adding additional knowledge over time for remediation for new expected threats. By automating its growing and highly specialized knowledge base for testing and by constantly adding new testing scenarios, this leading hedge fund's security is continuously improving. This best-practice deployment of continuous security validation helps the hedge fund's cyber defense team identify and prioritize remediation against the most pressing risks and threats.

The third and also highly important use case was to better and more objectively manage accountability between its cybersecurity team, the network operations team, and the information technology teams. Now they work together using the objective reporting from the BAS platform to identify gaps of concern, remediate those gaps, and validate that the remediation is performing as expected. This provides this leading hedge fund with the tools for audit necessary for expanded risk analysis and oversight reporting.

ATTACKIQ

U.S. Headquarters
9276 Scranton Road
Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com** and follow us on **Twitter**, **Facebook**, **LinkedIn**, and **YouTube**.