ATTACKIQ®

Case Study

Fortune 500 Asset Management Firm Empowers its Purple Team with the AttackIQ Security Optimization Platform

Few sectors come under such sustained attack from cybercriminals as financial services. According to figures from Boston Consulting Group, financial services firms are in fact 300 times more likely to fall victim to an attack than any other business.[1] These organizations are under constant threat of malware and security breaches, which can lead to huge reputational damage and in some cases highly punitive regulatory fines.

For one Fortune 500 asset manager headquartered in the U.S., the scale of the cyber threats makes ensuring its cybersecurity controls are purpose fit a high priority. The red team leader at the company puts it succinctly: *"Given our size, we have a pretty good budget to spend on security platforms. One of our chief challenges is therefore to ensure that these platforms do the job expected of them to a high standard."*

To help in this process, the company has integrated the AttackIQ Security Optimization Platform into its security operations. The large asset manager uses the platform primarily as a vehicle for the continuous and automated validation of its security controls, inclusive of firewalls, endpoint detection and response (EDR) systems, data loss prevention (DLP) systems, and antivirus security. In addition, the platform facilitates purple team operations — a security team structure in which members of blue and red teams work together collaboratively to achieve a threat-informed defense.

Automating Breach and Attack Simulation With AttackIQ

Before partnering with AttackIQ, the security team built testing and validation scenarios by hand. These manual processes were time consuming and error-prone, often falling short before any meaningful insights were achieved.

The complexity of the approach, as well as the associated drain on resources, meant that the firm ran tests and purple team exercises with far less frequency than it would have liked. A cybersecurity analyst from the company who is familiar with the project explains: *"Our manual process meant that it could take upwards of one to six weeks to get something across the finish line. And that was not always possible. Sometimes we would spend several weeks planning for how we would conduct the tests only to realize that our company doesn't allow that kind of testing in our network. We were wasting far too much time."*

Another challenge stemmed from the fact that the organization used a wide variety of operating systems, which required it to deploy different types of tests across its various platforms, therefore adding additional cost and complexity. The time had come to find a solution that is cross-platform compatible and able to execute validation assessments rapidly and continuously.

CUSTOMER

Fortune 500 Asset Manager

LOCATION

United States

INDUSTRY

Finance

HIGHLIGHTED SOLUTION AREAS

- Automated Testing and Team Enablement
- Control Audits
- Continuous Compliance Reporting and Dashboarding
- Security Pipeline Validation
- Threat Hunting
- Analyst Training and Certification
- Control Rationalization

BUSINESS IMPACT

- Enables the company to reduce the time it takes to prepare for validation exercises from up to six weeks to a matter of minutes
- Enables threat emulation and automated breach and attack response to help embed a threat-informed defensive posture
- Has identified weaknesses in the firm's security systems enabling them to be fixed
- Empowers purple teams with enhanced intelligence and reporting for greater impact
- Increased cadence of purple team exercises to one per month

[1] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

Having evaluated the options of the market, the security team at the company selected the AttackIQ Security Optimization Platform given its maturity and superior capabilities. AttackIQ's Security Optimization Platform realistically emulates adversary activity, enabling organizations to test their security program, while generating real-time performance data to improve their overall security posture.

Enabling Rapid and Continuous Validation

The company primarily uses the platform for two use cases. The first is for continuous validation of its security controls, which it can now run on a scheduled basis against a range of assets to determine its security posture. According to the lead cybersecurity analyst at the firm: *"Knowing that we can test our systems every week, and potentially every day, means we can be sure our controls are working as we would expect."*

> ***"Knowing that we can test our systems every week, and potentially every day, means we can be sure our controls are working as we would expect."***
>
> - Lead Cybersecurity Analyst, Fortune 500 Asset Management Firm

The second use case for the AttackIQ Security Optimization Platform lies in supporting purple team exercises. These exercises are conducted either to report to internal stakeholders on the cyber-readiness of the business, or to comply with SOC 2 (Service Organization Control) audits, which assess the ability of a business systems to protect data.

Empowering Purple Teams

With the AttackIQ Platform, the security team no longer needs to build validation scenarios manually. Instead, it can draw on the pre-built scenarios in the platform, which have been designed around real-world threat intelligence, leveraging the MITRE ATT&CK® framework of commonly used tactics and techniques to accurately mimic the activities of adversaries. This has enabled the company to dramatically increase the frequency of purple team exercises to one per month.

The company also uses the AttackIQ Vanguard service, which provides 24/7 continuous breach and attack simulation analysis, expert advice on how to optimize the AttackIQ platform and improve the defense capabilities that matter most, and support in investigating the potential for attacks on the firm's network. The Vanguard service proved invaluable in helping the company work out its deployment strategy and maximize its level of security coverage.

Accelerating Test and Validation Exercises

With the implementation taken care of, the firm could rapidly extract value from the platform. As well as improving the accuracy and relevance of validation scenarios, the solution saves significant time for the company. Rather than spending weeks developing each scenario, the security team can now launch them immediately, dramatically reducing the time to insight. The high levels of automation delivered by the platform also means that the purple team can focus on running the exercise rather than simply setting it up.

What's more, the platform approach means that the company no longer needs to waste time creating different tests for different assets. With AttackIQ, all relevant systems can be tested concurrently and continuously, reducing complexity, and saving yet more time.

A Strategic Fit

AttackIQ fits perfectly with the Fortune 500 asset manager's overall technology strategy, which is cloud-first and heavily focused on automation. As a result, it achieves significant benefits from the AttackIQ Security Optimization Platform.

During the initial phase of the COVID-19 pandemic, for example, the AttackIQ solution helped the company adapt to home working. The red team leader at the company explains it like this: *"At first it was difficult to maintain the cadence of operations as people took to their home offices. However, with AttackIQ, we had a platform that could continue the same levels of automated testing regardless of what was going on around it. That helped us establish a strong baseline and understand what was happening to key controls during this chaotic period."*

Identifying Potential Problems

In calmer times, the platform has proved to be a constant source of insights for the company, some of which have been rather surprising. One such surprise was around its firewall appliance, which constantly failed against the AttackIQ scenario tests because SSL (Secure Sockets Layer) encryption / decryption wasn't enabled. As a result of this insight, the company was able to properly configure the next-generation firewall capabilities inherent in its devices, inclusive of SSL encryption, which will greatly enhance its security posture.

Another example of the practical benefits of the AttackIQ Security Optimization Platform relates to the firm's EDR systems. The company uses different systems for its servers and its desktop devices and found challenges around deploying agents. AttackIQ enabled the firm to understand the differences between the two systems and where difficulties developed. The information enabled the firm to work with the EDR system vendors to remediate the issues and improve the performance of its systems.

Clarity of Communication

As well as identifying these and other issues, the AttackIQ platform provides the security team with clear intelligence that they can use to communicate with senior management. As the red team leader says: *"AttackIQ provides us with context so we can clearly explain the possible consequences of ineffective security controls. That enables us to get business buy-in and funding where change is required."*

> *"AttackIQ provides us with context so we can clearly explain the possible consequences of ineffective security controls. That enables us to get business buy-in and funding where change is required."*
>
> - Red Team Leader, Fortune 500 Asset Management Firm

In fact, the AttackIQ Security Optimization Platform enables the security team to create a range of different reports to suit the needs of various audiences. Following a purple team exercise, for instance, the platform enables the security team to export reports that are technical enough for incident response teams to understand the indicators of compromise, and the types of behavior exhibited in the scenario, while also enabling it to create reports better tailored to senior management; providing a quick digest so they can make informed decisions rapidly.

Keeping on top of the Platform

Throughout its partnership with AttackIQ, the asset manager has leveraged training and resources from the AttackIQ Academy. Everyone in the firm that uses the platform had been put through the academy's training courses so that they can use it to its full potential. Moving forward, the company plans to use new elements of the AttackIQ Security Optimization Platform, such as Attack Graphs, and will once again draw on the academy to ensure its people are trained and ready to go.

ATTACKIQ

U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat Informed Defense

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.