CASE STUDY: MSSP

Managed Security Service Provider (MSSP)

Executive Summary

This managed security service provider (MSSP) is a leading provider of managed IT and cybersecurity solutions for the financial services, health care, and payments industries. Specializing in hedge funds, private equity firms, and asset managers, the company has extensive experience supporting the alternative investment space. This MSSP offers a wide variety of services and has hundreds of employees and multiple key locations across the U.S.

> "We required a BAS platform with complete support for the MITRE ATT&CK™ framework. This would support and enhance our penetration testing services, which are offered to the most elite members of the financial services community. We required this platform to be customizable and highly extensible and to be able to support both our production systems and the production systems of our customers.
>
> AttackIQ's BAS platform met all of these goals over the past few months. AttackIQ allows our team to continually validate existing penetration test scenarios while continually adding new knowledge for current and evolving threat-based scenarios. It is a powerful force multiplier for our red teams to use. This is a win-win for us and our financial services customers."
>
> — MSSP Security Operations Team

The MSSP further wanted to expand the effectiveness and capabilities of its penetration testing services. This is a necessary and critical compliance deliverable for its clients in the financial services market.

The Challenge

This MSSP offers a vendor risk program, a service to address enterprise vendor management cybersecurity and compliance. The MSSP's vendor risk program helps clients regularly diagnose and manage the cybersecurity risk inherent in working with vendors, and it is architected based on industry best practices. The vendor risk program leverages a wide variety of interactive tools and reports, providing clients a 360-degree snapshot of where its vendors are at all times.

In growing its capabilities for penetration testing, this MSSP decided to build upon the MITRE ATT&CK framework and to operationalize it with a breach and attack simulation platform. It wanted to continually expand the testing, especially those tests that initially uncovered gaps, and run the expanding test suite to gain compound knowledge. This would offer its customers a unique advantage in ensuring that their current production systems were resilient and performing to expectations, as well as adapting quickly to the discovery of gaps in their defenses. The MSSP was absolutely resolute in its requirement to, if needed, support both penetration testing needs and the ongoing production system validation.

The Situation

The financial services industry is under constant attack from highly sophisticated cybercriminals and, in some cases, even nation-states. Recent data breaches show that cyber attackers have breached many financial institutions and successfully exfiltrated confidential personal information. Cyber attackers have also fraudulently diverted funds through breaches that exploited weaknesses in financial institutions' defenses, allowing them to breach and defraud financial application systems such as SWIFT. In most cases where systems were successfully breached, the primary attack vector was attributable to simple errors in administration and misconfiguration that gave rise to unintended but significant vulnerabilities.

Given the constant economic and competitive pressure and the high incentives to operate more cost-effectively, sophisticated financial firms such as hedge firms are allocating new resources with extreme care. Yet it is important that they do not miss opportunities to mitigate basic deficiencies in basic operational processes, security control configuration, and security control selection. This MSSP's penetration testing services can rapidly highlight areas of risk. In the financial services industry, this is sometimes due to overburdened system administrators inadvertently creating vulnerabilities.

The Solution

AttackIQ's BAS technology allowed the MSSP to codify and automate its existing red team penetration testing capabilities. The MSSP's red teams can now automatically emulate the full attack and expanded Kill Chain against enterprise infrastructure using AttackIQ's software agents and virtual machines. This has enabled the MSSP to find the performance gaps in customer production deployments, strengthen its security posture, and work to continually validate that remediation is in place

AttackIQ's BAS platform assessed readiness and validated that the MSSP's customers' security controls are performing as originally intended. Automation enables the AttackIQ platform to work autonomously and to scale to meet new requirements.

The MSSP was able to rapidly implement the BAS platform. The scenario testing library is substantial and well-aligned with MITRE ATT&CK, so the MSSP was also able to easily customize the scenarios to meet specific customer needs.

Outcomes

The primary use case is to support the red team testing needed to meet financial industry compliance requirements. The AttackIQ BAS platform has enabled this MSSP to validate cyber readiness continuously and at a low cost that makes it compelling to add to its services bundle for most of its customers. The automation of the platform and the existing testing content library help the MSSP keep penetration testing costs low and efficacy high.

This MSSP's investment in AttackIQ has been well rewarded. The objective assessment of security control performance, identification of gaps, and validation of remediation have enabled the MSSP to meet the most complex and demanding customer requirements. The MSSP's teams can immediately identify configuration errors, advise customer blue teams to implement necessary changes, and confirm that the changes as implemented are correct. The MSSP is also satisfied with the selection of the MITRE ATT&CK framework and considers this a key part of the BAS solution.

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**.