CASE STUDY: NON-PROFIT FINANCIAL INSTITUTION

Non-Profit Financial Institution

"We're pleased with the vision and direction of the AttackIQ breach and attack simulation (BAS) platform. AttackIQ provides a comprehensive automation platform with a SaaS agent-based deployment architecture, a broad and diverse scenario library, and an open architecture. All of this gave us a fast time to value. We've used the platform for over three years, and we're looking forward to how the product will evolve further into compliance reporting and risk management."

Executive Summary

This non-profit emergency financial assistance organization was incorporated as a private nonprofit organization in the early twentieth century. The organization has collected and distributed donations in the form of scholarships, grants, and loans. It has collected and distributed over $1 billion in aid in the past decade alone.

Non-profit Financial Institution

In the face of increasing targeted threats towards organizations of its type, it became essential to this financial organization to better understand if its cybersecurity infrastructure could protect it against the most likely threats it might face. After considerable evaluation of the alternatives, it chose MITRE ATT&CK™ as the primary cybersecurity framework for its team to use to make these assessments and AttackIQ as the BAS platform to operationalize these capabilities.

The Challenge

This organization was seeking a way to use BAS automation to give assurance of its security controls' effectiveness and performance. A BAS platform would also provide data on the effectiveness of its security policies and the performance of its personnel. The BAS platform was also intended as a readiness tool to prepare the institution for the various third-party oversight security tests that would be meticulously performed by red teams. This non-profit organization's mission is to distribute as much aid as possible, so it was important to the organization to test and evaluate the technology first and then keep the associated expenses as lean as possible to minimize the overhead costs.

The government also offers value and shared services that this organization could leverage for security, but the organization felt that it needed to be innovative and resourceful enough to accomplish its security goals without being another tax on government operations.

The Situation

In support of its mission, this non-profit financial organization must manage the privacy data of over 1.5 million U.S. citizens. For this and other reasons, the business-critical systems that the organization uses to support its operations are classified under NIST 800-53 as a moderate sensitivity system.

This organization was initially introduced to AttackIQ several years ago through Patrick Gray's Risky Business Podcast (with the City of San Diego's CISO Gary Haislip as a guest speaker) and thought Breach and Attack Simulation (BAS) was an investment worth exploring.

In the deployment of any BAS platform, it was important to work within the existing resources available at the organization, to achieve rapid return on investment, and to meet mission objectives. Any selected vendor partner needed to implement the technology rapidly, with minimal disruption, and to assist the organization's security team in achieving success with visible milestones and near-term goals.

The Solution

AttackIQ's BAS technology allows this financial organization to automatically simulate the full attack and expanded Kill Chain against enterprise infrastructure using software agents, virtual machines, and other means. This large depth and breadth of capability allow for continuous validation of the its security program. This enabled the organization to find its performance gaps, strengthen its security posture, and improve overall incident response capabilities. AttackIQ's BAS platform assessed readiness and validated that the organization's security controls are performing as originally intended. Automation enables the AttackIQ platform to work autonomously and to scale to meet future requirements.

AttackIQ's BAS also provided essential support for live production environments. Small changes to configurations or administration can open new vulnerabilities in the organization's cyber defense. This is the ever-present gap between test environments and live production environments that, undetected, could compromise operations. For this reason, the organization's live production environments are subject to the same Kill Chain of emulated activities that an attacker would seek to execute.

This non-profit relief organization was able to implement the BAS platform rapidly. The scenario testing library is broad and capable, so it was able to implement rapidly out-of-the-box. Important scenarios for the organization included credential caching, as well as email, web, and DNS exfiltration scenarios. It was straightforward to align these with the organization's MSSP's responsibility.

Outcomes

First and foremost, AttackIQ enabled the organization to validate cyber readiness continuously at an exceptionally low overhead cost. The automation of the platform and the existing testing content library help the non-profit organization keep costs low and in alignment with its budgets. Key use cases of the organization that were successfully implemented are validating the controls that protect the inappropriate access and exfiltration of sensitive privacy data and validating that financial distribution processes are effective and secure.

This organization has also used the testing as a way to technically validate that proper procedures are being used with password storage and related management. This would not be possible without the AttackIQ platform. The organization has also experienced good results in simulating attacking the technical environment as an adversary would to ensure that the contracted managed security service providers (MSSP) are effective and capable in response to incident response service-level agreements (SLAs). In addition, the organization was also able to use the AttackIQ platform to help validate end-user training compliance awareness and internal security response protocols.

This organization's investment in AttackIQ BAS has paid off well. Its most recent third-party penetration test noted that the organization has "excellent security practices and a textbook cyber defense." This was due, in part, to the rigor and completeness provided by AttackIQ's BAS platform.

AttackIQ also helped the organization with immediate risk reduction. The platform identified unexpected gaps in endpoint logging functionality and helped the organization identify some areas that were at risk to potential WannaCry attacks due to the continued use of SMBv1. AttackIQ helped the organization close the loop on this asset/configuration management issue and drive remediation of that asset through a staged and careful process.

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**.