CASE STUDY: LEGAL PROFESSION

Law Firm

Executive Summary

This leading international law firm has offices throughout the United States, Europe, Asia, and the Middle East. It provides services in dozens of countries and provides over 100,000 pro bono hours annually.

This law firm's commitment to a secure cyber environment reflects its connection to the issues affecting the community in which it works as well as to its clients. The firm feels that it is vital to deploy a cybersecurity program to meet and, where possible, exceed industry best practices. In order to do this, it wanted to increase real-time visibility into the performance of the security controls in its production systems.

> "The increasing cyber threat against the legal profession, and the highly sensitive and confidential data that we must manage on a daily basis, requires constant alignment with cyber defense best practice. The MITRE ATT&CK™ framework offers a better way for us to organize all of our efforts, and the operationalization of MITRE ATT&CK by the AttackIQ breach and attack simulation (BAS) platform enables us to better understand and reduce our risk in many areas."

Law Firm Cybersecurity Operations

This law firm decided to operationalize its efforts around MITRE ATT&CK and chose AttackIQ as the BAS platform to support this effort. It was highly important to the law firm's cybersecurity team that it could accurately review the performance of its security controls, understand the gaps, and make the best data-driven decisions to close those gaps and reduce risk. It also wanted objective reporting that it could use to assess risk in a measurable way that could then be reported to its senior management team.

The Challenge

In 2018, a panel at the American Bar Association Annual Meeting in Chicago raised concerns that U.S. law firms might be failing to comprehend the full threat, vulnerabilities, and consequences of cyber attacks from around the globe. The consensus of the panel was that cyber attacks are inevitable and that preparation for law firms was necessary to avoid not only the hardware issues but also the post-attack consequences.

This law firm has worked diligently to build best practices into its cybersecurity strategy in every possible area. The law firm's cybersecurity team wanted immediate visibility and awareness of new gaps in its defenses, especially those accidentally introduced by changes in configurations in any part of its network.

The law firm's team also decided that it wanted this capability operationalized around MITRE ATT&CK, which it believed offered an organization and structure well suited to both its current and future security planning. The team wanted to move aggressively to meet and reduce new sources of cyber risk, and it felt that one of the best ways to do this was to select and implement a BAS platform.

The Situation

This law firm must defend and secure the information technology infrastructure for over 1,000 lawyers and advisors across the globe. Global compliance requirements drive many of the baseline requirements that the cybersecurity team must measure, align with, and validate. Given the global scope of the organization and the need for strict adherence to compliance regulations, both the facilities and the local personnel have varying requirements for application and network access that must be supported securely in the local environment.

The legal profession has seen a continuing increase in cyber threats and reported incidents annually. This is especially true in many of the countries in which this law firm serves.

The Solution

AttackIQ's BAS technology allows the law firm to automatically emulate the full attack and expanded Kill Chain against enterprise infrastructure through a broad variety of means. The AttackIQ BAS platform allows for the continuous validation of this law firm's security program. The law firm is now better able to identify and remediate gaps, strengthen its security posture, and improve overall incident response capabilities.

The AttackIQ BAS platform also assesses readiness and validates that this law firm's security controls are performing as intended and required. Automation enables the AttackIQ BAS platform to work autonomously and to grow as required to meet future needs.

AttackIQ's BAS platform has also proven essential in providing support for the live production environments that the law firm considers critical. Changes to configurations or administration can create new vulnerabilities in the law firm's cyber defense. This gap between test environments and live production environments could compromise the firm's operations if not promptly detected. The AttackIQ BAS platform has been implemented so that all of the law firm's production environments are subject to the same Kill Chain of emulated activities that might be leveraged by a cyber attacker.

Outcomes

The initial implementation of MITRE ATT&CK and the AttackIQ BAS platform went into production in early 2018. This law firm runs chosen and customized baseline scenarios on a regular basis and has tied the AttackIQ platform to its weekly and monthly red team assessments. The BAS platform has become an indispensable part of consistent and repeatable red team activity and of validation of remediation of the gaps identified by the red team.

Several use cases have found high value to the law firm, as they do to other customers. These include continuous security validation, MITRE ATT&CK operationalization and alignment, validation of security controls, and close integration with the red team mentioned above. All of these use cases have been successfully addressed, and, as a result, critical gaps have been identified and remediated, performance has been improved in targeted areas, and the initial return on investment to the firm has been provided through both reduced costs and reduced risks.

This law firm has also used the technology in lockstep with current threat analysis data. It utilizes many sources of real-time threat analysis and ties that into its cybersecurity program planning, activities, and remediation. The BAS platform has enabled it to move rapidly from the identification of a new and likely threat to an objective assessment of the efficacy of its cyber defenses to mitigate the threat decisively.

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**.