ATTACKIQ®

Solution Brief

AttackIQ® Provides Vital Security Control Validation and Strategic Decision Support in Health-Sector Organizations

AttackIQ® Provides Vital Security Control Validation and Strategic Decision Support in Health-Sector Organizations

Against a backdrop of increasing cybersecurity risk — particularly ransomware and concurrent data exfiltration — CISOs in healthcare and public health (HPH) organizations are investing hundreds of billions of dollars in cybersecurity. Much of this is going to security controls that protect critical clinical and administrative systems, data, and networks.

To demonstrate a return on your investments and obtain ongoing funding for your security program, you need to accurately assess the efficacy of your security controls against the attacks that are likely to affect your organization.

The AttackIQ Security Optimization Platform helps you do just that. It gives you the most consistent, trusted, and safest way to test and validate security controls at scale and in production. Using a threat-informed approach to breach and attack simulation that is based on the tactics, techniques, and procedures (TTPs) detailed in the MITRE ATT&CK® framework, AttackIQ enables you to:

- Identify and prioritize relevant cyberadversaries and threats;
- Emulate adversaries by simulating the techniques they would use to attack your controls;
- Identify gaps that may exist in your controls; and
- Verify that mitigation efforts are successful through ongoing testing.

AttackIQ can be used by your security operations-focused blue teams, by red teams, and by your compliance and governance staff. AttackIQ's dashboards and reports are designed not only to facilitate the work of each of these groups, but also to help you communicate your security optimization efforts clearly to executive leadership and the board.

ROBUST, EASY TO IMPLEMENT, SAFE FOR PRODUCTION

- The AttackIQ management system can be deployed remotely as software-as-a-service (SaaS) or directly on-premises. AttackIQ agents are lightweight and easy to install.
- AttackIQ does not need dedicated test points, making the platform dramatically more scalable than other solutions.
- Because AttackIQ agents have a low profile, there is little risk that they will expose your production controls to real adversaries.

Three Critical Things to Do with AttackIQ

Below are a few examples of how different teams in your organization can leverage AttackIQ to expose security gaps, demonstrate the effectiveness of attempts to remediate those gaps, and verify assumptions about human and technology performance. To review AttackIQ's 26 data-driven, threat-informed solutions, visit attackiq.com/solutions.

Expose Undetected Threats Through Automated Testing

As the recent SolarWinds breach has shown, leaving security controls unexamined can enable security breaches to fester, causing significant damage. Electronic health records (EHR) are a particular source of concern: a breach of one health plan's EHR system lasted nearly a year and a half and affected over 9.3 million people, costing the company more than $5 million in fines for HIPAA violations.[1] With AttackIQ, your security team can set up automated scripts to regularly exercise the security controls protecting the EHR data, using known adversary techniques that are likely to target that data.

[1] "Excellus Resolution Agreement and Corrective Action Plan," hhs.gov, January 15, 2021

Expose Undetected Threats Through Automated Testing (cont.)

HPH organizations have also found AttackIQ to be more effective for evaluating the proficiencies of its blue teams, compared with sporadic, manual performance testing. AttackIQ focuses testing on likely adversary behaviors, rather than checking performance specs and configurations against compliance benchmarks. This motivates blue teams to proactively seek proof of efficacy rather than rely on the assumption that their controls will work as long as they comply with certain standards.

Objectively Evaluate New Security Controls and MSSP Offerings

If you have identified a need for new investments in security technology, stakeholder buy-in is critical. A third-party, objective validation of each vendor's performance claims is more compelling than vendor spec sheets and other claims.

During vendor proofs of concept, the AttackIQ platform can exercise each of the proposed solutions against benchmark attack scenarios to help you determine which technology performs best in meeting your security requirements. You can also use AttackIQ to compare the effectiveness of commercial and open-source security solutions. And you can perform similar evaluations of managed security service providers (MSSPs) in the pre-sales stage.

Reduce Cyberrisk Before and During Mergers and Acquisitions

Despite — or perhaps because of — the COVID-19 pandemic, merger and acquisition (M&A) activity in the healthcare sector is continuing unabated. According to a recent survey of healthcare CFOs, 31 percent said they plan to acquire physician practices, 28 percent plan to merge with another organization, and 17 percent plan to acquire another organization.[2]

If your organization is among those engaging in M&A activity this year, you can use the AttackIQ Security Optimization Platform to test the cybersecurity controls of companies you intend to onboard. This analysis will enable you to determine the level of cyberrisk the new organization will generate and identify areas of improvement in advance of the deal closing. During each phase of the onboarding process, iterative simulations of likely attacks may reveal potential gaps that result from the consolidation of the two organizations' IT infrastructures, as well as discrepancies in processes and proficiencies between the blue teams of the merging organizations.

A Healthier Approach to Risk Management

Successful cyberrisk management requires a long-term commitment to keep pace with the evolution of our adversaries. As part of a holistic approach to risk management, the AttackIQ Security Optimization Platform can help you and your stakeholders make data-driven, threat-informed decisions about how to protect your healthcare or public health organization. AttackIQ also invests continually in improving the industry-leading automated BAS capabilities that underpin the Security Optimization Platform and in educating the security community through the AttackIQ Academy. Please visit attackiq.com to learn more and to schedule a demonstration of AttackIQ for your organization.

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 identify 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 MITRE Engenuity's Center for Threat Informed Defense.

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

[2] "2021 BDO Healthcare CFO Outlook Survey," BDO USA, 2021