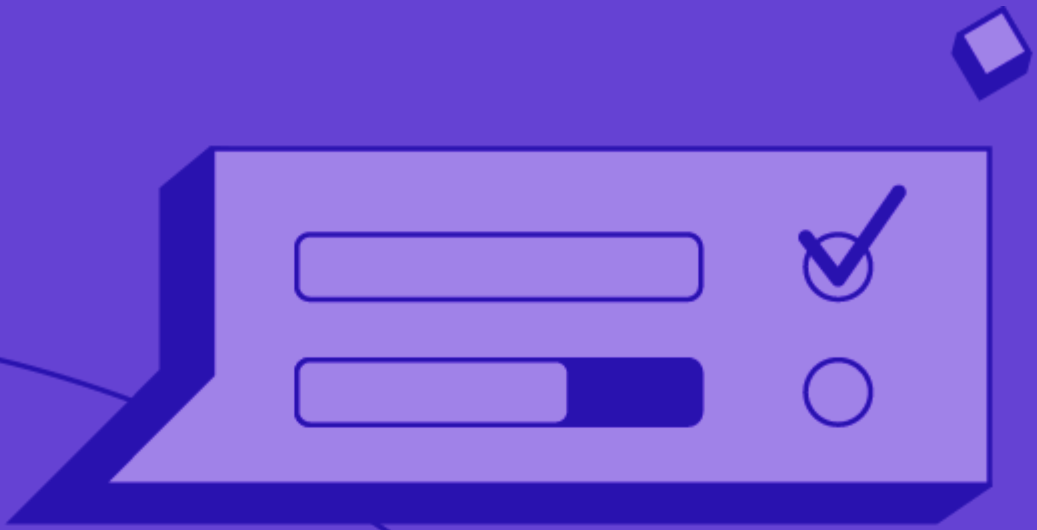
ATTACKIQ®



Case Study

Automated Attack Simulations Build Healthcare Technology Firm’s Confidence in Network Protections

A healthcare technology firm had made a name for itself by overcoming the numerous obstacles to establishing innovative new businesses in the pharmaceutical space. When its new information security (infosec) architect came on board, she knew she would have to muster the same resolve to prevailing over the company's cybersecurity hurdles.

At the time, the company was a startup and the security program was fairly immature. "*We had an attitude of wanting to be ahead of the curve and to utilize cutting-edge technologies,*" she reports. "*At the same time, as a startup, the business was very focused on reaching the finish line without paying too much attention to infosec. I noticed right away that we weren't performing any control assessments or vulnerability scanning.*" The company did not have access to red team resources, either internal or external, so the security architect began evaluating her options for closing this gap.

"*That's when I came across the attack simulation industry, which fit right in with our attitude and strategy,*" she says. "*We didn't want to just use vulnerability scanning software to look for a predefined list of weaknesses. The idea of real attack simulations was very appealing, because we saw that they could provide more of a real-world experience.*"

Why AttackIQ?

The security architect evaluated several top players in the breach and attack simulation (BAS) space and conducted proofs of concept for a few of them. The AttackIQ Security Optimization Platform stood out for several reasons. She found the user interface to be intuitive and appreciated the platform's out-of-the-box integrations with the firewall and endpoint security solutions that the company uses. "*Compared with the competition, AttackIQ offered more integrations with other solutions we already had in place,*" she says.

She was also impressed with the size of the pre-built scenario library in the Security Optimization Platform, which meant streamlined deployment of simulations across a wide range of potential attacks: "*AttackIQ had a bigger selection of simulations than any of the other BAS systems we considered. We also liked that some of the scenarios are editable. Users can choose whether to run a scenario as an administrator or a regular user, and whether to run it out of the user directory or the system directory. We can also use our own files in the prebuilt simulations.*"

> *"Using the Security Optimization Platform is like having an extra person on staff to do whatever penetration testing we need."*
>
> - Information Security Architect, Healthcare Technology Firm

The possibility of running simulations of custom-built scenarios was appealing, as well. "*We really liked the option to custom-code scenarios in AttackIQ,*" the security architect notes. "*We haven't done that yet, but we intend to hire programmer interns to write scenarios specific to our situation. We immediately saw that AttackIQ would not only solve our immediate need through the massive library of scenarios, but also give us limitless room to expand the assessments. That flexibility was a big driver of our decision to go with AttackIQ.*"

CUSTOMER

Healthcare Technology Firm

LOCATION

Switzerland

INDUSTRY

Healthcare

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Investment Decision Support
- Mergers and Acquisitions

PROJECT BUSINESS IMPACT

- Confidence throughout the organization that crucial control gaps have been closed
- Unbiased and data-based justification and prioritization of cybersecurity investments
- Greatly enhanced responsiveness to executive team requests for information about protection against specific types of attacks
- Reduced security risk for returning subsidiaries, by identifying control gaps before they are merged into the corporate IT infrastructure
- Comprehensive penetration testing regimen deployed with minimal staffing impact

Vulnerability Revelations Lead to Better-Informed Investments

The proof of concept (POC) made the choice clear, and the company began rolling out the Security Optimization Platform. The security architect developed a testing strategy as her team worked through the AttackIQ POC, so, once the purchase was complete, they were able to deploy the solution and set up a series of routine simulations within just a few weeks.

"*One thing I've really loved about AttackIQ is that it's very easy to use,*" she says. "*It took all of 10 minutes for me to figure out how it works and how to use it. And for the few issues I have had, the AttackIQ support team has provided amazing response. The platform has been flawless for us, and we have no complaints whatsoever.*"

The three-person infosec team began building a regime of monthly control testing aligned with the MITRE ATT&CK framework. The security architect is impressed with the way MITRE ATT&CK highlights threat areas that might not have otherwise been on the company's radar.

> "*That first AttackIQ report was a reality check. It showed a whole host of threats that we were vulnerable to and were previously unaware of.*"
>
> - Information Security Architect, Healthcare Technology Firm

"*As an example, if we failed a test of our data exfiltration scenarios, that would raise concern not only about an external attacker exfiltrating data, but also about insider threats,*" she says. "*MITRE ATT&CK enables us to look at our environment as a whole and see problems throughout the attack chain. Could somebody on the inside escalate their permissions and move laterally to machines we thought were segmented on another network? Maybe we're good at securing initial access but we're terrible when it comes to privilege escalation. MITRE ATT&CK phrases all these connections in an understandable way, so that we can truly see the full cadence of any prospective attack.*"

In addition to the MITRE ATT&CK framework that is built into the security optimization framework, the healthcare technology company brings in some of its own threat intelligence, including a feed from the Health Information Sharing and Analysis Center (H-ISAC) intelligence community.

The first control assessments that the infosec team performed were eye-opening. "*We had security controls that were comparable to other businesses of similar age, size, and maturity,*" she says. "*But that first AttackIQ report was a reality check. It showed a whole host of threats that we were vulnerable to and were previously unaware of. The process raised some eyebrows and gave impetus to our drive to install more controls. We were able to prevent people from doing some of the weird things they had previously been doing that created infosec risk, like storing confidential information on USB drives or sending sensitive files to personal devices.*"

Revealing Gaps and Justifying Corrections

Now, the company runs around 500 attack simulations each month. These scenarios are designed to test the company’s preparedness to defend against ransomware and against attacks on the firewall, endpoint protection, or data loss prevention (DLP) controls. When an assessment reveals a gap, the security team uses that information to support needed changes.

> *“We’re more likely to free up budget for a specific solution if we can demonstrate that certain types of attacks can currently execute in our environment because we don’t have that solution in place.”*
>
> – Information Security Architect, Healthcare Technology Firm

“*Sometimes closing a gap may be as easy as tweaking a group policy,*” she says. “*Other times, we might need a new endpoint DLP solution. The AttackIQ reports help us see, at a glance, where our weaknesses are and what projects we should prioritize. Having proof of a control gap also helps drive the ROI [return on investment] determination for a project. We’re more likely to free up budget for a specific solution if we can demonstrate that certain types of attacks can currently execute in our environment because we don’t have that solution in place.*”

When using the results of a simulation to justify implementing a new technology or tactic, the security architect will subsequently run an ad hoc assessment to make sure the change has effectively closed the control gap. “*That is bringing us a lot of value,*” she reports. She also uses the Security Optimization Platform to run ad hoc scenarios in response to concerns raised by management.

“*Frequently when an attack on another organization makes news headlines, upper management and the board want to understand whether we’re protected against that particular threat,*” the architect says. “*We can go in and run one-off simulations, then reassure the executive team by showing them how our systems perform in an assessment that’s close to what’s happening in the wild. Using the Security Optimization Platform is like having an extra person on staff to do whatever penetration testing we need.*”

There’s one more use case for which the company is leveraging the AttackIQ platform: to safely integrate business units into the corporate security infrastructure. Some of the company’s subsidiaries have developed their own separate IT teams, then changed their mind and returned to the corporate fold. “*They come back home and want us to take care of them,*” the security architect reports. “*We will test their environment to see what has been opened up and how secure their network is. AttackIQ helps us make those evaluations and figure out whether there are any control gaps we need to close before bringing them back into our network.*”

Cybersecurity cures may not always be easily accessible. But at least, for this healthcare technology company, routine simulations through the AttackIQ Security Optimization Platform are enabling a clear and comprehensive diagnosis of every control problem. For an organization committed to beating down barriers, that is a step in the direction of assured survival.

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.