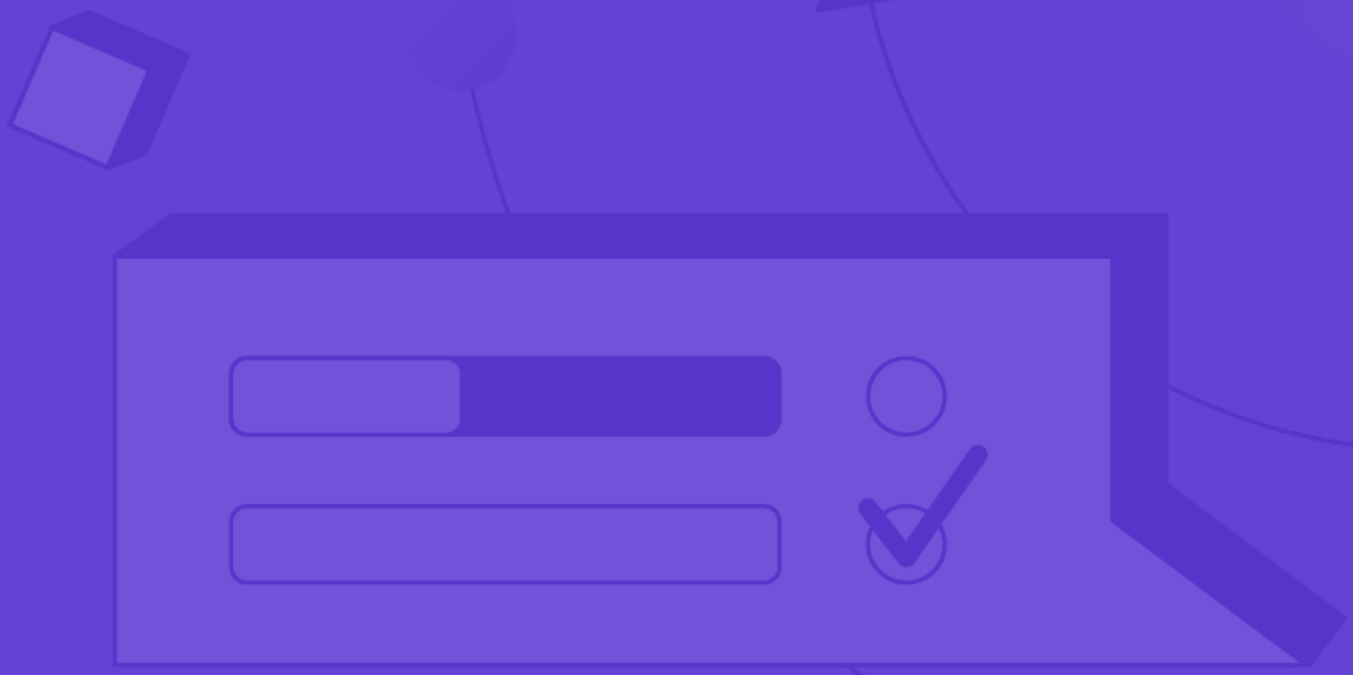
ATTACKIQ®

Case Study

Leading Biosciences Company Demonstrates Security Control Effectiveness and Reduces Insurance Premiums Using AttackIQ



Insurance companies want to know that you have everything you need to keep your house from catching fire. In cybersecurity, insurance is an extremely tough market. Cyberinsurance companies now say annual insurance assessments aren't enough. They want to know how well security programs are working and to see verifiable data from monthly, weekly, and even daily reporting to prove the effectiveness of their client's security controls. Security teams are responsible for answering endless questionnaires, and their responses significantly impact the company's premiums.

For a leading biosciences company, their cyberinsurance underwriter threatened to take away the company's insurance if the security team could not at a minimum annually demonstrate the effectiveness of their security controls. When the Director of IT Security at the company was asked by his legal department to answer a complex questionnaire for their cyberinsurance, he immediately thought of one platform to help prove that the company's security controls were doing what they said they were.

"When the hard questions were given to me through legal, I looked for a solution to back up my position, and AttackIQ was the first true solution that popped into my mind, and it worked."

- Director of IT Security, Leading Biosciences Company

Demonstrating Effectiveness to Insurers

"The insurance questionnaires went from very basic onboarding and generic controls questions, like, 'do you have a firewall? do you have an endpoint protection solution in place?' to complex questions that were far beyond traditional insurance questions that were even difficult for me to answer," he explains. The complex questions ranged from "what framework are we leveraging as a basis for the CSIRP [cyber security incident response plan] and have you ever had a breach, and can you validate or provide evidence to suggest your position?"

"We used AttackIQ and pointed it towards the firewall or even our filer, which houses our intellectual property and a lot of sensitive employee data, to validate that our permissions and controls are doing what we say they are," explains the Director of IT Security. "First, I leveraged it as a basis for my response. Then I provided documentation and evidence to legal to support my position."

"It was very technical reports like validating technical controls, almost like simulating an external or internal pentest on our critical systems like firewalls and data repositories, endpoints, etc. It was a validation tool for us," he shares.

CUSTOMER

Leading Biosciences Company

LOCATION

Americas

INDUSTRY

Biosciences

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Security Control Rationalization

BUSINESS IMPACT

- Enables security team to manage security risk better
- Saves millions of dollars by providing control effectiveness to a major insurance underwriter
- Augments the need for a full-time red team and outsourcing red team activities

Reduces Insurance Premiums

With the audible evidence from the AttackIQ Security Optimization, the biosciences company's legal department could negotiate a lower premium with the cyberinsurance company. "It did produce a good result for the company. First, in retaining our existing insurance, where the premiums continue to go up, and the market is very tight. Second, we had threats of losing our insurance without demonstrating adequate controls at a minimum annually." shares the Director of IT Security.

> *"You must answer truthfully to the best of your knowledge and not put yourself at risk by answering incorrectly. We leveraged the AttackIQ Security Optimization Platform to find the answer we were looking for, and to either share or have that documented in case of a breach, and we were held accountable for those responses."*
>
> - Director of IT Security, Leading Biosciences Company

Founding the Biosciences Company Cybersecurity Practice

The Director of IT Security has been with the leading biosciences company for about six years and started in a leadership role for the datacenter and network operations. "After much effort in redesigning and scoping our datacenter, network, and WAN operations for global expansion, I leveraged that experience to find our cybersecurity practice," he explains. "We've been a full bore for about three years. We're relatively new in the maturity model but growing fast in FTEs, controls, and influence across the organization."

The cybersecurity team is relatively small, with four team members. The Director of IT Security describes the team's strategy as "blue team and defense driven. We're proactive in getting ahead as much as possible to be those blue team defenders for the organization. Preventing breaches and responding to typical IDR SOC platforms, but without the benefit of a red team," he explains.

That's where the AttackIQ Security Optimization Platform comes in. "It's a great platform to mature your security program very quickly, especially in a tight industry where you may not have the budget to expand and grow your program as quickly as you'd like through FTE expansion and adding additional analysts."

"AttackIQ was really the best of breed. There was no question that it was the right choice for us after leveraging the free resources through the Academy. AttackIQ is invested in the community and expanding the knowledge to cybersecurity professionals. There's much value and integrity in that. I look forward to this in partnerships." he explains.

"We leverage AttackIQ Academy as an onboarding process for new hires. Both current analysts have gone through every training module and certification. It's a great training resource. Finding a solution like AttackIQ, where we can train our existing staff and augment the need for full-time red team practitioners on board, is huge."

"We have no intention to build a dedicated red team because we have AttackIQ in place. AttackIQ provides me and my team, broader knowledge of the landscape, and a platform we can leverage to simulate. That is huge. AttackIQ augments the need for a full-time red team or even outsourcing red team activities in the traditional, almost legacy sense these days," explains the Director of IT Security.

"It's a huge opportunity for us and other companies to get these tools in your hands that are exponentially more expensive to put in place through traditional means. Breach and attack simulation with AttackIQ is our best investment in maturing our program."

- Director of IT Security, Leading Biosciences Company

Instilling Confidence in the Board — Leading to a Promotion

"Going from having no security program to now reporting to the board quarterly, having actionable intelligence, and auditable reporting to validate that our controls are doing what we say they do. One, it helps us from a budget perspective because it instills confidence in the board that we are investing our dollars wisely and getting the results we promised. I did get a promotion after this. I went from senior manager to a director-level position," explains the Director of IT Security.

When pulling actionable intelligence for the board, the Director of IT Security uses AttackIQ to simulate a ransomware attack and share effectiveness percentages. "I look at percentages of how effective we were able to prevent a breach, specifically ransomware. That metric is huge. Ransomware network security breaches and cloud assets are always in the news. Ransomware is the largest one every quarter. I'm asked the question — have we ever had a ransomware outbreak? And how prepared are we to prevent one if there were to be one?"

"For example, I'll take the LokiLoker ransomware outbreak, simulate that attack, and tell the board that we could show you exactly what would happen if we were to be attacked with that ransomware, and here's how effectively we are at preventing it," explains the Director of IT Security.

Immediately Reveals Cost Savings

Once the AttackIQ Security Optimization Platform was deployed, the leading biosciences company immediately started seeing business benefits. "Initially, we leveraged AttackIQ in several ways. From demonstrating the efficacy of our existing controls, maturing our controls, OS imaging, and vendor validation," says the Director of IT Security.

The Director of IT uses AttackIQ to demonstrate the efficacy of existing controls and even saved significant costs during an XDR validation (extended detection response). "We leveraged AttackIQ for breach and attack simulations against our incumbent XDR provider," he explains. "There was cost saving involved because we were able to demonstrate that our existing solution was more effective than these much more expensive alternatives that came to the table with many promises," says the Director of IT Security. "Based on our AttackIQ results, we could maintain that existing vendor relationship, and it's been successful."

"When we can prove that our solutions and controls are not just adequate, but they're rock solid, there's much value there. The investments in our firewalls, endpoint controls, and network security controls help build the program's reputation and instill more confidence. Then when we go to the board for requesting a large sum of funding for maybe a new project, there are not as many questions,"

- Director of IT Security, Leading Biosciences Company

The biosciences company recently acquired a biotech company out of the U.K. "In that global expansion, we intend to leverage AttackIQ for GDPR validation for those endpoint assets, cloud resources, etc. Beyond the traditional scope that we're used to traditional in our United States-based business and operations," says the Director of IT Security.

Most recently, the security team is "leveraging AttackIQ to harden our OS images for endpoint deployments. With a large remote workforce having a solid concrete image is important. We take that responsibility off the deployment team to manually make configuration changes, etc. We can bake that into that deployment model."

Building for the Future, Confidently

"Our company has one of the largest biotech campus buildouts underway. We expect to be complete in 2024, but part of that is network design and security being the primary responsibility of my team. When we spin up this brand-new network, and with new technology, a lot of which is new to our team, that will help harden our network security posture. We'll leverage AttackIQ to validate our controls and have auditable documented results," shares the Director of IT Security.

As the security team adds more responsibilities, they will find additional use cases for the platform and continue to increase confidence at all company levels that its security controls will hold up well. "We have a good way to go with the maturity of the AttackIQ platform. Being a relatively small team, we still need to balance out our red, blue, and purple team exercises with daily operation responsibilities. But it is the platform we leverage for a better understanding of the network and overall security posture. AttackIQ provides supporting documentation and evidence that we are doing what we say we are." That supporting documentation — and all the data behind it — gives him and his team an increased level of confidence in their overall security program performance.

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 plan 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 the MITRE Engenuity's Center for Threat Informed Defense

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