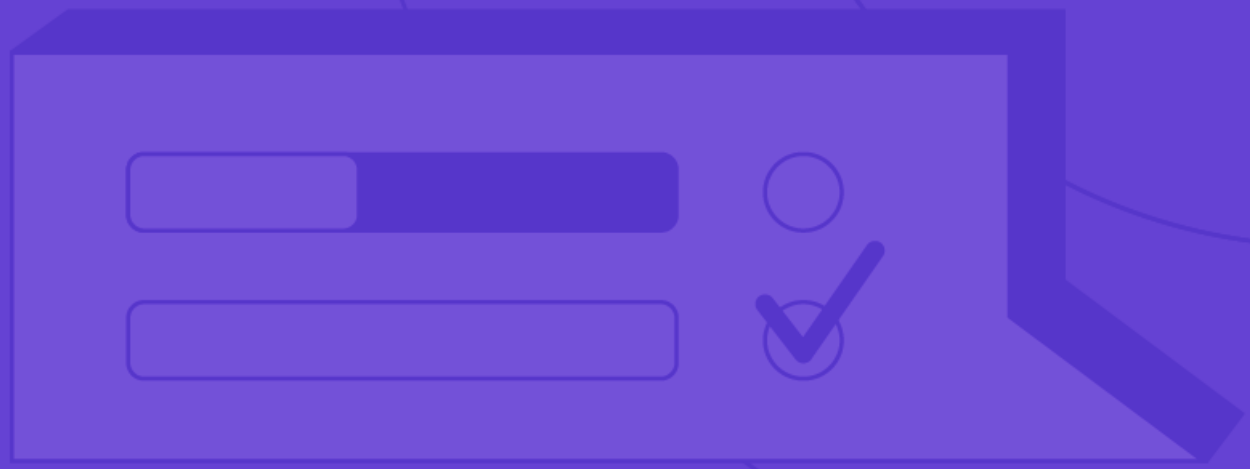
ATTACKIQ®

Case Study

# A Fortune 50 Retailer Relies on AttackIQ for Automated Security Control Validation Against Real-World Threats and Optimized Overall Cybersecurity Program Effectiveness



Fortune 10-500 companies have a vast attack surface, and as threat actors become more advanced, it's becoming extremely tough for these companies to stay ahead of threats. According to figures from Cyberpion's 2022 research analysis , Fortune 500 companies contain an average of 148,000 critical vulnerabilities. As new vulnerabilities are exposed, security teams invest in the best-of-breed security solutions to close gaps.

A Fortune 50 retailer's mission is to deliver the right products with the best service. They must do so by protecting customers and corporate data from the possibility of being breached. For one Fortune 50 retailer with over 2,000 stores in the U.S. and Canada that serves approximately 19 million customer transactions per week, security is a crucial focus for the company.

The Lead Information Security Analyst for the Offensive Security team is responsible for finding and remediating vulnerabilities for the Fortune 50 retailer. He calls his cybersecurity strategy a *"no-nonsense security framework."* The Lead Information Security Analyst likes to keep it to a simple method by asking himself, *"what is the problem, and what can we do to fix it?"*

The Offensive Security Group at the company is a relatively small team of about 8-10 members. *"My team's daily responsibilities are to find vulnerabilities within the enterprise and work with various teams to bring forth remediations,"* he says. *"We also do inside consulting with other teams to make sure their security protection and response systems are working properly."*

# The Road to Breach and Attack Simulation

The Lead Information Security Analyst saw an opportunity to automate security control testing with a breach and attack simulation (BAS) platform. *"Breach and attack simulation was relatively new to the security industry and a way to automate testing with limited team resources,"* he says. *"It's easy to have testers and defenders, but once you start drilling down into specific threats and TTPs, it's not super easy,"* he explains. *"Anybody that wants to get ahead of the curve should invest in automation with a breach and attack simulation platform like AttackIQ."*

Another reason why the Lead Information Security Analyst also wanted to invest in breach and attack simulation was because of a team resources issue. *"The whole issue that we faced was a team size issue,"* he explains. Breach and attack simulation helped him augment his defensive teams by finding gaps in the organization's defenses and helping the team quickly close gaps to improve cybersecurity effectiveness.

**CUSTOMER**

Fortune 50 Retailer

**LOCATION**

United States

**INDUSTRY**

Retail

**SOLUTION AREAS**

- Automated Testing and Team Enablement
- Security Strategy and Investment Decision Support
- Threat Hunting

**BUSINESS IMPACT**

- Increased confidence in security control's effectiveness for the organization
- For emerging threats, rapid answers about whether existing controls can detect and prevent them
- Valuable Offensive Security Group team resources can focus on emerging issues and support for control improvements rather than running routine manual tests
- Increased EDR detections by ~30%

# Why AttackIQ?

The Lead Information Security Analyst began evaluating breach and attack simulation (BAS) tools throughout the market. During the evaluation process, he particularly liked the interface and the intuitiveness of the Attack Security Optimization Platform. *"What set AttackIQ apart was how intuitive the platform was. Other BAS tools that we tested were convoluted and all over the place."* When selecting a BAS platform, he wanted more than a tool but a long-term relationship with a vendor he could trust. *"AttackIQ wasn't just a tool, but a long-term partnership with the people at the company. Everyone I interacted with was great with customer service and knew the platform well, which was important to me,"* he explains. *"My interactions with the employees made it clear that AttackIQ was a good company I could trust."*

> *"Anybody that wants to get ahead of the curve should invest in automation with a breach and attack simulation platform, like AttackIQ."*
>
> - Lead Information Security Analyst, Offensive Security Group, Fortune 50 Retailer

# Bringing the Offensive and Defensive Security Teams Together

After deploying the AttackIQ Security Optimization platform, the Offensive Security team could now provide the organization with additional data on the effectiveness of their security controls that they previously lacked. *"Now, we can automatically test something and get feedback within the AttackIQ. Nobody needs to check for alerts manually. We brought automated testing to different teams, like for our blue and networking teams, for networking segmentation."*

The Lead Information Security Analyst saw an opportunity to adopt a purple teaming approach. *"For the longest time, we didn't have a purple team. It wasn't until we got more into AttackIQ that I went to my manager and suggested the purple team approach."* In a purple team construct, *"we attack, and another team fixes. That's the only way we'll be able to get some traction,"* he explains.

*"Since adopting the purple team approach, we have had a good cadence with the blue team, where we meet and share reports from the AttackIQ dashboard. We are way more engrained than we used to be before we had AttackIQ."*

# Benefits of AttackIQ

The Fortune 50 retailer uses the AttackIQ Security Optimization platform to validate its security controls continuously. According to the Lead Information Security Analyst, *"our initial intention is to ensure whatever endpoint security solution we have, that our technology stack is firing appropriately,"* he explains. *"That it's catching when it's supposed to catch, preventing what's supposed to prevent. AttackIQ has allowed us to test and get a good picture of our EDR capabilities."*

The Lead Information Security Analyst was able to measure the success of AttackIQ because the detections have increased since deployment. *"I know AttackIQ is working as intended because the detections have increased. We are up around 30% for our detections."*

Another way the company uses the Attack Security Optimization Platform is to test the company's firewall technologies for the network security team. *"The network security teams would be considered a customer of ours because of the big firewall manufacturers they use. It's nice to be able to test those routes and rules to make sure things aren't getting through the network."*

> *"The ability to test scenarios that recently hit the news is a huge relief and extremely beneficial to know that your company is protected. We used AttackIQ's scenarios for Log4j and the Ukrainian conflict. I'm always grateful that AttackIQ is in the war rooms at short notice. We can trust AttackIQ to share content from recent cyberthreats, and it's awesome when these releases come out because I can tell people we already tested that."*
>
> - Lead Information Security Analyst, Offensive Security Group, Fortune 50 Retailer

# Alignment with MITRE ATT&CK Framework

With the AttackIQ Platform, the Offensive Security group no longer needs to build validation scenarios manually. Instead, they can pull from the pre-built scenarios in the platform, leveraging the MITRE ATT&CK framework of commonly used tactics and techniques of real-life threat actors.

*"MITRE ATT&CK has been an enormous resource for us,"* the Lead Information Security Analyst explains. *"We use it a lot with AttackIQ because we aren't just concentrating on our EDR baselines. But there are known TTPs that specifically target similar industries to us. We use the MTIRE ATT&CK framework to determine what to go after and what to test next."* The Offensive Security Group also benefits from AttackIQ's attack graphs, which emulate the adversary with specificity and realism to test their cyberdefense technologies against multi-stage attacks.

# Testing with Realism Against Advanced and New Threats

AttackIQ responds within 24 hours to a U.S. government Computer Emergency Response Team (US-CERT) alert with an initial assessment and blog for our customers to test their security posture against emergent threats. *"The ability to test scenarios that recently hit the news is a huge relief and extremely beneficial to know that your company is protected,"* the Lead Information Security Analyst explains. *"We used AttackIQ's scenarios for Log4j and the Ukrainian conflict. I'm always grateful that AttackIQ is in the war rooms at short notice. We can trust AttackIQ to share content for recent cyber threats, and it's awesome when these releases come out because I can tell people we already tested that."*

# Increased Confidence in the Company's Security Readiness

Moving into 2023, the objective of the Offensive Security Group remains the same, protecting the company from any security vulnerabilities that would interfere with delivering the best service to their customers. The Lead Information Security Analyst's goals for this year are to expand AttackIQ's security reports to the companies' C-suite to show that they are sufficiently protecting their customers' data in order to increase confidence in security effectiveness. The goal: *"To give information and data for the company that they didn't have before, so that we can make better educated decisions and strategic changes that will further enhance our tech stack and improve our overall security posture."*

ATTACKIQ®

U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com