SafeBreach

Fortune 500 Healthcare Provider Establishes Continuous Security Improvement with SafeBreach

As the largest not-for-profit healthcare insurance provider is entrusted with vital information, which needs to be secured at all times. For the security team, the charter was to establish adaptable defenses that could safeguard systems, data, and services against constantly evolving threats and vulnerabilities. To achieve these objectives, the team turned to SafeBreach.

Challenges

The Fortune 500 Healthcare Provider is the region's largest not-for-profit healthcare insurance provider. They have been around for more than 80 years, and have grown to serve nearly one million subscribers.

Within the organization, the security team is responsible for safeguarding the organization's systems and services, as well as a range of sensitive data, including financial records, personally identifiable information, protected health information, and more.

In order to advance the organization's safeguards, several years ago, the team began to evolve its approach, moving to establish a stronger, more defensive posture. Rather than solely targeting compliance requirements, they sought to take a more holistic, proactive approach to guard against the most critical threats and ensure their defenses would evolve as those threats evolved.

Challenges.

For the security team, threats are evolving constantly—and so are the environments that need to be protected. The team needed to ensure effective defenses were in place at all times.

Solution.

The team employed SafeBreach to execute safe, automated cyber attacks, so they could rigorously, continuously validate their security controls.

Benefits.

With the solution, the team can gain the critical insights they need to strengthen their defenses, boost the security team's maturity, and establish more consistent, efficient operations.

The team wanted to build effective threat models, understand in detail where their vulnerabilities really were, and take proactive steps needed to reduce their overall attack surface. They started by taking a look at systemic issues, asking several fundamental questions:

- **Do we see what we need to see?**
- **If we see something, are we sure we know what to do about it?**
- **How do we measure our effectiveness?**

Early on, they would do penetration testing on an annual basis. However, these tests typically failed to uncover any issues, and team members weren't convinced that the results were conclusive. They also subsequently employed a red team to aggressively wage attacks and discover vulnerabilities that could be exploited. These exercises helped shape a lot of the thinking about how to defend the organization.

Over time, however, they knew they needed to do more, more consistently.

"Just because we have controls in place doesn't mean they're working, and our security posture is changing all the time," said the CISO at the Fortune 500 Healthcare Provider. "A mistaken configuration change in a VPN service could open up a new vulnerability at any time. That's why it's so vital to continuously validate our tools and overall security posture."

That's what led the CISO and his team to start looking at using automated, safe attacks to validate security controls. They needed to establish a way to continuously validate whether the controls in place were working, discover any vulnerabilities that attackers can exploit, and continually fine tune their defenses.

Solution

To strengthen security, the team chose to employ the SafeBreach platform. The SafeBreach platform can do automated testing of the team's security architecture, using advanced, patented technology that can execute attacks safely and continuously.

Compared to the alternatives they had evaluated, SafeBreach was much easier to implement and use. Alternatives required a lot of time and effort to stitch things together, and staff had to manually build all attacks.

"SafeBreach already had a library with a lot of attacks," the CISO revealed. "You could press the button and start running."

He continued, "My team loves the SafeBreach platform. We have agents running on premises and in the cloud, and we're continuously running the solution. We rely on the platform extensively to generate different reports that we can use to communicate with management. The platform provides the vital insights that enable us to continually fine tune our defenses."

Use Cases

They implemented the platform years ago, and have continued to expand the ways in which the solution is used. The following sections offer an overview of some of the key ways the platform is being employed today.

Solution

Threat Assessment

SafeBreach runs all of the activities associated with advanced cyber attacks, sending and opening emails, detonating payloads, triggering alarms in simulators, and so on.

They're able to run advanced attacks that are composed of a number of steps, and assess each phase in detail. The team gets US-CERT alerts from SafeBreach Labs, which help them manage ongoing threat assessments.

For example, they may find out about a heightened level of threat from a nation-state. Based on what they know about the actor, and their tactics, techniques, and procedures, the team can wage similar attacks, test their defenses, and assess whether there are vulnerabilities that the actor could exploit.

Mock Scenario Training

"Our staff changes occasionally, but what's even more challenging is the fact that everything else is changing constantly, including malware, tactics, and environments," the CISO explained. "We wanted to establish continuous training, so teams would always be best prepared to respond when issues arose."

With SafeBreach, the team can do mock scenario training to ensure staff are prepared to respond to the latest threats.

Tool and Service Validation

With its robust capabilities, SafeBreach helps the team vet the efficacy of the solutions they implement, which was difficult to do in the past. For example, if the team employed a new anti-malware tool, and the vendor claimed to catch 90% of malware, how could they tell whether that was true? How could they track exactly how it worked in their specific environment? With SafeBreach, the team can test and validate the efficacy of the tools they have in place, and hold their vendors accountable for the claims and commitments they make.

With SafeBreach, during proof-of-concept phases, the team can test products to validate that they work as advertised. In addition, they rely on a managed security service provider to operate their network operations center, which is staffed on a 24-hours-a-day, 7-days-a-week basis. They use SafeBreach to verify whether operations staff are following up according to established policies when events occur.

A Long-Term, Ongoing Partnership

Over the course of the deployment, the teams and SafeBreach have established a partnership, working together to advance the deployment and solution capabilities.

"Over the years, SafeBreach has responded to a number of requests and input we've provided, including adding support for the MITRE ATT&CK framework, offering more flexibility in running specific attacks, and providing increasingly robust integration with the Cortex SOAR solution," the CISO said.

Before implementing SafeBreach, the team looked at doing security control testing manually, but ultimately realized that, in order to meet their objectives, they'd need to take an automated approach. With SafeBreach, they've been able to harness automation so they can execute attacks safely and continuously.

Longer term, the teams wants to establish a self-defending infrastructure. Instead of having team members responding when alerts arise, they wanted to start employing orchestration and automation of responses, so they could handle incidents more quickly and consistently. Through the solution's integration and automation capabilities, SafeBreach is helping the team execute on this longer-term vision.

"People often think about security in binary terms, focusing on whether they're winning or losing," the CISO stated. "When it comes to security, you need to stay in the game—at all times. We need to be focused on defense constantly, that's why we're continuously training and improving."

Benefits

By using the SafeBreach platform, the team has been able to realize several key benefits:

Boost Team Maturity

By harnessing the solution to do mock scenario training, the team is able to refine their expertise, workflows, and policies. With SafeBreach, the team can establish the continuous training that helps ensure team members are optimally prepared for the latest threats.

Strengthen Safeguards

SafeBreach has delivered the insights that enable the team to identify gaps and weaknesses before they're exploited. Now, they proactively report to senior leadership about breaches in the news, the security team can assess whether the Healthcare Provider is exposed to the same risk, and, if so, take steps to mitigate it. By revealing the gaps that can actually be exploited, SafeBreach is helping teams more intelligently prioritize their remediation efforts.

Efficiency and Consistency

With SafeBreach, the Healthcare Provider doesn't need to have multiple people spending a lot of time running manual tests. This frees staff up to focus on more strategic efforts on an ongoing basis. Further, the automation of test execution ensures that testing is more consistent, which yields significantly improved insights.

SafeBreach

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

Learn More

If you're interested in learning more about how SafeBreach can benefit your organization, be sure to visit [call to action, TBD].

CTA

