SafeBreach

CASE STUDY

SafeBreach Makes Mock Scenario Training Real for Fortune 500 Biopharmaceutical Company

Learn how the security team for one of the world's largest biopharmaceutical companies moved beyond the limitations of tabletop exercises by leveraging SafeBreach to execute highly realistic, hands-on training scenarios to improve security skills and efficacy.

Industry Biopharmaceutical

Challenge To stay in front of fast-moving business dynamics and security threats, ongoing staff training was vital for the biopharmaceutical company's security team. However, verbal tabletop exercises offered limited value in strengthening staff skills.

Solution The organization's CISO deployed SafeBreach to run mock scenario exercises based on real-world events.

Results With SafeBreach, the security team can conduct far more realistic, hands-on training exercises, helping the organization achieve:

- Improved team training processes and enhanced capabilities
- Greater operational efficiency and consistency through automation
- Data-driven insights for strengthening safeguards

The Limits of Tabletop Exercises

The Fortune 500 biopharmaceutical company develops innovative medicines for life-threatening illnesses. To fulfill their mission, teams across the organization rely on a vast array of sensitive, highly valuable intelligence. Consequently, the company has to guard against a variety of threats, including ransomware and intellectual property (IP) theft.

The security team is responsible for safeguarding a wide range of highly valuable systems and data, including financial reports, patient and employee records, clinical trial results, and more. Given the critical, complex nature of the organization's security profile, it is important not just to test technology, but to verify the effectiveness of people and processes, and to guard against misconfigurations that are so often the cause of vulnerabilities and breaches.

"Just because teams have a security tool in place doesn't mean the organization is safe," said the organization's CISO. "Headlines abound of cases where security teams within enterprises aren't using tools effectively. For example, a tool may be indicating there's a problem, but staff are ignoring it."

To keep staff at the top of their game, ongoing training is crucial. Previously, the team used tabletop exercises to help test and train staff. During these exercises, a leader would read from a script, and players in the room would talk through and demonstrate their approaches to respond to the outlined scenario.

Based on this setup, the training exercises proved to be limited and more theoretical in nature. They also didn't give specific insights into how processes, tools, and people worked in practice. While staff shared high-level approaches, they didn't get specific training and practice into what they needed to do, such as the specific tools they needed to use and how.

"There's a big difference between driving a car and doing a driving simulation," said the CISO. "People came into our tabletop events knowing it was an exercise, and often they weren't taking it seriously enough."

The Power of Real-World Scenarios

To enhance their mock scenario training, the team wanted to leverage a tool that could create a real incident. This would give staff something tangible to respond to and enable far more realistic training exercises. After conducting an extensive evaluation of tools available, the team chose to deploy SafeBreach.

Using advanced breach and attack simulation (BAS) technology, the SafeBreach platform can perform automated testing of an organization's security architecture. The solution enables the team to run simulated exercises that can be used for mock scenario training.

With SafeBreach, the CISO's team has been able to take training exercises to the next level. Instead of having staff verbally talk through scenarios, they use SafeBreach to execute real-time scenarios based on real-world attacks. SafeBreach offered the team at the Fortune 500 biopharmaceutical company several key advantages:

An Extensive, Flexible Playbook

With SafeBreach, the team has been able to leverage a playbook to establish all the steps in an entire exercise. The solution offers comprehensive threat coverage, featuring capabilities for simulating ransomware, nation-state attacks, and more. The solution can simulate the attack chain from end to end, including sending an email, opening it, detonating a payload, and triggering alarms in simulators. Finally, the platform obfuscates the activity, meaning analysts involved in exercises can't tell the event was generated by SafeBreach, making simulations work more effectively.

Consistent, Repeatable Scenario Execution

By using SafeBreach to automate attack simulation, the team saves significant time. Plus, the implementation of automation helps ensure far more consistency than having multiple staff members doing a lot of manual tasks. SafeBreach agents intelligently scale and are equipped to automatically determine what attacks to run on which simulators. Not only does this ease the burden on the security team, but it helps remove bias as well.

Flexibility to Support a Range of Use Cases

Given the solution's flexibility, the team was able to rapidly expand the ways the solution was used. With SafeBreach, they're able to validate security controls, investigate the security of potential acquisition candidates, conduct red team exercises, run testing to reduce tool sprawl, and more.

Ongoing Benefits & Improvements

By employing SafeBreach to execute their mock scenario training, the security team at the Fortune 500 biopharmaceutical company has been able to realize a range of benefits:

Boosted Team Maturity

SafeBreach has proven indispensable in improving team training and optimizing their capabilities. With SafeBreach, the team can identify and reduce speed bumps in its processes and validate the controls of the technologies it has in place. As the CISO explained, “When it comes to time-critical efforts associated with incident response, ensuring the ‘muscle memory’ of our people is critical. With SafeBreach, we can give teams the hands-on practice that ensures they’ll be most effective when real events arise.”

Improved Efficiency & Consistency

With SafeBreach, the team can boost operational efficiency by streamlining and automating many ongoing, low-level tasks. As a result, the team can spend more time focusing on strategic efforts, including automating the execution of indicators. Ultimately, with these capabilities, the team has been able to significantly improve consistency, which helps enhance training and ongoing insights.

Greater Insights for Strengthening Safeguards

Through SafeBreach, the team can effectively test its people, processes, and technologies. By executing more advanced mock scenarios, team members have been able to improve their understanding of how the security operations center (SOC) functions and help boost overall security awareness. Now, when staff hear about breaches in the news, they can quickly assess whether their environment is exposed to the same risk. The solution reveals gaps that can be exploited, helping the team identify the vulnerabilities they need to prioritize first.