SafeBreach

CASE STUDY

SoftServe Inc. Stays on the Cutting Edge of Cyber Threat Detection & Response with SafeBreach

Learn how SoftServe leveraged the SafeBreach platform's breach and attack simulation capabilities for automated security control validation and discovered additional use cases that provided a whole new level of value from their BAS program.

softserve

Industry Software Development

Challenge In order to provide their global organization with a more comprehensive level of protection, the SoftServe security team needed to move beyond the limited and point-in-time insights of typical security validation tools like penetration testing and red teaming.

Solution SoftServe utilized SafeBreach to implement a solution that automated security testing of their corporate security controls, helping their security team stay on the leading edge of detecting and responding to the latest threats.

Results With SafeBreach, SoftServe achieved:

- Valuable insights into the effectiveness of security controls and overall security posture
- Diverse simulation types that enabled testing of both on-premises and cloud environments
- A unified place to collect security events and complete in-depth analysis of security control response
- The ability to support additional, value-add use cases including:
  - Identifying and fine-tuning security control misconfigurations
  - Testing and comparing different security solution vendors
  - Analyzing and adjusting endpoint protection rules and policies

SoftServe is a premier IT consulting and digital services provider. They have over 10,000 employees in 59 offices across 16 countries—and their customer base is just as robust and geographically diverse. For Michael Kropyva, associate vice president of information security at SoftServe, providing the vision and leadership necessary to manage the cyber risks associated with that type of global presence is of utmost importance.

Mr. Kropyva leads a sophisticated Cybersecurity Operations Center (CSOC) team responsible for developing, implementing, and monitoring a comprehensive enterprise cybersecurity and IT risk management program. His team works closely with the SoftServe IT infrastructure team, GRC team, and other corporate functions to implement the organization's full scope of cybersecurity controls, ensure business alignment of security initiatives, and support the overall security of the organization.

While Mr. Kropyva and his team utilized more traditional security validation practices like red teaming and penetration testing, they often experienced challenges with testing against the latest threats in a timely way, insufficient automation of testing on various platforms, and an inability to easily compare test results. In order to be successful, Mr. Kropyva knew his team needed a more continuous process for detecting and responding to emerging threats, testing security controls, and validating the team's response processes.

An Education in BAS: **Surveying the Vendor Landscape**

Mr. Kropyva first learned about breach and attack simulation (BAS) technology—and the potential benefits it could offer his team—through a report by analyst firm Gartner. He and his team then engaged in a bake-off of sorts, comparing several BAS vendors based on their level of maturity and their performance on key parameters, including:

- Availability of behavioral-based simulations
- Complexity of configuration and product exploitation
- Availability of integrations with existing security controls
- Flexibility of the attack simulation and their customization
- Release rate for newly discovered attacks and threats
- Reporting possibilities
- Recommendations on leveling identified threats

As the pioneer in the BAS space, SafeBreach came out on top. Not only is the platform backed by a world-renowned threat research team, it also has an extensive playbook with over 30,000 attack methods—including behavioral-based simulations—and the widest MITRE ATT&CK coverage in the industry. The playbook is also updated with new content within 24 hours of relevant US-CERT and FBI Flash alerts, allowing Mr. Kropyva and his team to confidently stay ahead of emerging threats.

The enterprise-readiness, ease of attack customization, and wide array of off-the-shelf integrations offered by SafeBreach meant SoftServe could get up and running quickly and seamlessly share simulation results with its existing security controls.

To top it off, SafeBreach's detailed reports provided SoftServe with valuable insights into the effectiveness of security controls, highlighting misconfigurations and opportunities for fine-tuning. And, as the platform's reporting capabilities continued to evolve, SoftServe would be able to leverage unique reporting on aspects like peer benchmarking, executive-level insights, and more.

The Evolution of the SoftServe BAS Program: **Landing and Expanding**

When Mr. Kropyva first engaged the SafeBreach team, his goal was simple: implement a continuous, automated process that could test the efficiency of SoftServe's security controls and identify misconfigurations.

During the onboarding process, Mr. Kropyva and his team defined a desired list of operating systems and networks that they wanted to test against attack simulations. The SafeBreach Support team provided recommendations for the most efficient placement of agents and network simulators to achieve the result they were looking for. Mr. Kropyva initially utilized SafeBreach-developed attack content both on a scheduled basis for regular security control validation and on a continuous basis to test against imminent threats. His team also leaned on SafeBreach's 24-hour guarantee to publish new attack content in response to relevant US-CERT and FBI Flash alerts.

> "It has been very helpful to be able to monitor threats published by CISA and immediately obtain information via the SafeBreach platform about the response of our security controls."
>
> **Michael Kropyva**
> **AVP of InfoSec, SoftServe**

When technical problems came up, the SafeBreach Support team promptly provided a solution or engaged the SafeBreach Product team to ensure appropriate changes were addressed in future versions of the platform. In addition, SoftServe received regular updates from the SafeBreach Customer Success team about product improvements, new functionality, and usage recommendations they could utilize to make the most of their deployment.

Fast-forward three years and SoftServe is an avid SafeBreach customer. They now have an automated solution they can depend on to test their corporate security controls, helping their team stay on the cutting edge of detecting and responding to the latest threats. The SafeBreach platform's diverse simulation types for on-premises and cloud environments provides comprehensive coverage of most of the scenarios Mr. Kropyva and his team need to protect against. The detailed reports provide an understanding of the efficiency of different security controls and illuminate misconfiguration and options for fine-tuning. The platform's integrations have proven highly valuable as well.

> "The integration points that the SafeBreach platform offers with other security solutions is a huge differentiator. This allows us to collect all security events in one place and complete a detailed response analysis of the reaction of implemented security controls against various types of malicious activities, which has been a game changer for us."
>
> **Michael Kropyva**
> **AVP of InfoSec, SoftServe**

Now, Mr. Kropyva has expanded his team's use of the SafeBreach platform to support additional use cases beyond just traditional security control validation, providing SoftServe with a whole new level of value from their BAS program.

USE CASE #1

Network Rule Misconfiguration

SoftServe deployed the SafeBreach network simulation tool within a segregated network environment to conduct ongoing assessments of security controls. This allowed for continuous evaluation and testing of the effectiveness of the network's security measures and protocols. SoftServe is extremely vigilant in ensuring its firewall network configuration is robust. SafeBreach makes that task simpler and even more rigorous.

SafeBreach sends simulation results to SoftServe, which in turn analyzes the data and take appropriate actions.

USE CASE #2

Security Vendor Solution Comparison

SoftServe used the SafeBreach agent simulation tool to thoroughly evaluate and test the efficiency of different endpoint security controls. This comprehensive assessment provided valuable insights into the robustness of its security solutions in defending against potential breaches.

During the assessment of endpoint security controls, the SoftServe team used multiple testing scenarios to carefully evaluate the effectiveness and reliability of the security measures in place. After completing the testing, SoftServe was able to make a data-backed final decision regarding the further use of the evaluated security controls, based on the comparison of the controls' response results.

USE CASE #3
Adjustment of Endpoint Protection Rules

As part of working with the SafeBreach platform, SoftServe used specific scenarios to evaluate the performance of security controls and configured policies at endpoints. Their goal was to conduct a detailed assessment of these measures to ensure the controls and policies were highly effective for strengthening the company's security infrastructure.

After thoroughly analyzing the test results, SoftServe was able to develop customized rules and security policies to effectively address the known endpoint security risks associated with protecting their systems and increase effectiveness of their endpoint controls.

Looking to the Future

Going forward, SoftServe will continue to leverage the SafeBreach platform to test their corporate security controls, but they have also seen the value BAS can provide beyond this traditional use case. Overall, their experience underscores the need for organizations with complex security environments to leverage tools like BAS that provide accurate, actionable insights to effectively navigate the ever-changing security landscape with confidence—and to be thoughtful and methodical about how they do it. Mr. Kropyva's advice to other organizations contemplating BAS technology? You may need to start slow, but you will not regret getting started now.

> "Implementation of a BAS program is a process, but one that will pay huge dividends in the future. Begin by implementing the BAS scenarios gradually—move from one security control to another and start testing critical systems. Based on the simulation results, you'll begin to develop new procedures and automations that will dramatically change the way your security team operates."
>
> Michael Kropyva
> AVP of InfoSec, SoftServe