SafeBreach

CASE STUDY

SafeBreach Helps Fortune 500 Biotechnology Company Establish Continuous Security Control Validation Across IT and OT Environments

Learn how this leading firm leveraged SafeBreach Validate to continuously identify and remediate security gaps across their IT and OT environments to address the challenges of an increasingly remote, global workforce.

Industry	Healthcare/Biotechnology
Challenge	In order to ensure a more comprehensive level of protection for remote workers during the COVID-19 pandemic—and continuing with an on-going hybrid work model—this Fortune 500 biotechnology company needed to move beyond the limited and point-in-time insights of typical security validation tools like penetration testing and red teaming.
Solution	SafeBreach Validate & SafeBreach-as-a-Service
Use Cases	▪ Security Control Validation ▪ Security Tool Evaluation ▪ Configuration Drift Tracking ▪ Site and Policy Comparison
Results **With SafeBreach, this Fortune 500 biotechnology company was able to:**	Quantify the effectiveness and efficacy of its security controls, including both preventive and detective tools Ensure adequate visibility and coverage for the latest IOAs, TTPs, and IOCs of US-CERT alerts, especially those targeting remote workers Emulate threat actor behaviors to test and improve their threat detection analytics and security control responses, as well as understand opportunities for lateral movement and infiltration/exfiltration by an adversary Develop a more structured approach to identify and remediate security gaps, including a monthly cadence for attack simulation testing across their IT and OT environments Support a data-driven EDR vendor comparison

This global Fortune 500 biotechnology company is responsible for developing and commercializing life-transforming medicines that address some of the world's most serious diseases. They have over 15,000 employees and serve customers across North America, Europe, and Asia. When the COVID-19 pandemic began, it was critical to empower their employees to continue their impactful work without the need to visit a brick and mortar office. But managing the cyber risks and closely monitoring the effectiveness of security controls for a highly distributed, remote and hybrid workforce would be critical.

Operationalizing CISA Alerts

In early 2020, the Cybersecurity and Infrastructure Security Agency (CISA) encouraged organizations to adopt greater cyber security measures to protect against the risks associated with remote work options becoming prevalent due to the COVID-19 pandemic. Soon after, the agency began to issue alerts specifically for phishing, malware, and other malicious activity targeted at remote workers.

This Fortune 500 biotechnology company's Senior Director of IT/OT knew their team needed an efficient way to validate whether the security controls they had in place were effectively protecting their remote workers against the threats outlined by CISA. Up to that point, their team relied on more basic tactics like implementing control configuration best practices, completing visual inspection of control configurations, and performing manual testing and troubleshooting. But these processes were time consuming, inefficient, and resulted in a significant amount of data to manually correlate and analyze.

The Senior Director of IT/OT sourced feedback from the CISO community to understand how other organizations were addressing these unique challenges—several peers recommended the **SafeBreach exposure validation platform** and its breach and attack simulation (BAS) capability, **SafeBreach Validate**.

As the pioneer in BAS, SafeBreach stood out based on its extensive playbook that boasted over 30,000 attack methods and the widest MITRE ATT&CK coverage in the industry. More important was the speed at which the playbook was updated with new content—SafeBreach's world-renowned threat researchers update the platform within 24 hours of relevant US-CERT and FBI Flash alerts. This would give the Fortune 500 biotechnology company's security team a crucial edge, allowing them to confidently stay ahead of emerging threats targeting their remote workforce. The SafeBreach platform was the clear choice.

Critical Support & Onboarding Services

During the onboarding process, the organization worked closely with the SafeBreach team to ensure they could achieve the results they were looking for. This included identifying the ideal network locations for simulators, installing agents, configuring firewalls and security tools, tweaking the associated security rules, and understanding best practices for using the SafeBreach platform.

The Fortune 500 biotechnology company also took advantage of the **SafeBreach-as-a-Service** (SBaaS) program, which provides on-going strategy and support from SafeBreach's elite team of exposure validation experts. Through this engagement, they were able to develop and implement 28 different integrations between the company's infrastructure and the SafeBreach platform via a custom data feed.

This proved instrumental in helping them operationalize the platform and see a clear—and immediate—enhancement of their ability to assess the effectiveness of the security controls they had in place to protect the company and its remote workers.

Continuous Testing Across IT & OT Environments

Now, the Fortune 500 biotechnology company has over 50 simulators strategically deployed across its IT and OT environments and has established a monthly cadence for attack simulation testing of both. They complete ad-hoc testing as new content is added to the platform based on US-CERT and FBI Flash alerts and—depending on the alert type—complete IT to OT and OT to IT testing as well.

They leverage out-of-the-box and custom dashboards to help them tell the story about the test results to the rest of the organization, and utilize the SafeBreach platform's Insights feature to support remediation. Multiple service towers within IT have partnered with the Senior Director of IT/OT to ensure they are maximizing their use and ROI of the SafeBreach deployment and simulations. And as the deployment of the SafeBreach platform has continued to expand into multiple environments, it has resulted in greater communication and cooperation between different business units.

Expansion to Additional Use Cases

Based on the strong return on investment the Fortune 500 biotechnology company saw from its initial SafeBreach engagement, they were eager to explore the potential for deeper value using SafeBreach to select a new endpoint detection and response (EDR) solution. They needed a surefire way to understand how well each tool would perform under real-world circumstances within their environment, and weren't in a position to simply take the vendors' word for it.

The teams quickly came together and created a plan for an in-depth and lengthy "proof of value" validation process aimed specifically to test the detection capabilities of multiple vendors against coordinated simulations designed to mimic real-world attacks.

During the course of this testing, SafeBreach experts noticed that one vendor was not blocking a set of common but potentially dangerous and well-documented attacks. The security team worked quickly to investigate the anomaly and identify that this was a symptom of a critical misconfiguration within the EDR technology. The Fortune 500 biotechnology company shared the SafeBreach simulation results and analysis with the EDR vendor's technical representative, who quickly addressed the policies within the technology and confirmed once the policy in question had been updated. SafeBreach and the company's security team coordinated a new set of tests, leading to drastically improved detection results.

With the assistance of SafeBreach technology and expertise—and with indisputable, empirical evidence of the competing controls' efficacy in detecting and responding to a multitude of threats—the Fortune 500 biotechnology company was able to make a highly informed decision to implement multiple high-scoring EDR vendors to work in concert for the security of the company's critical operational technology network.This EDR evaluation was fundamental to their ability to protect the organization, its users, and their data.

Looking to the Future

As this Fortune 500 biotechnology company continues to change and grow, they envision their use of the SafeBreach exposure validation platform to do the same. In the immediate future, they plan to incorporate email attack simulation testing, but also have a long-term review process to see where else the platform can provide value.

What advice does the Senior Director of IT/OT have for other enterprise organizations looking to begin their exposure validation journey with SafeBreach?

1. Work to understand your internal environment, which will help you implement the SafeBreach simulated environment.
2. Set clear goals with each of the teams that will be involved and work towards operationalizing the platform in collaboration with all stakeholders.