ICON Validates Security Controls With SafeBreach

Global provider of drug development solutions and services uses breach and attack simulation to quantify risks and validate security.

SafeBreach

SafeBreach

CHALLENGES:

ICON wanted to more quickly and consistently identify security risks, and provide assurance that security protections were working in a highly regulated environment.

SOLUTION:

ICON deployed SafeBreach to simulate thousands of attacks from the Hacker's Playbook™ automatically, continuously and safely. The platform provides a "hacker's view" of ICON's enterprise security posture to proactively predict attacks, validate security controls and improve SOC analyst response.

BENEFITS:

- Able to validate SOC alerts and response times and provide comprehensive metrics to management on security
- Achieved complete kill chain visibility into infiltration, lateral movement and exfiltration
- Achieved continuous, automated and faster validation of security defenses for entire infrastructure

"Because we run the SafeBreach platform continuously to assess risks, we use simulation data as the security metrics for our leadership team. Simulations deliver a highly comprehensive view about the state of our security because the SafeBreach Playbook includes all types of attacks – infiltration, lateral movement and exfiltration. When we are asked about new attacks or risks, SafeBreach helps answer these questions."

– Tony Clarke, Head of Information Security, ICON plc

ICON plc [NASDAQ: ICLR] is a global provider of drug development solutions and services to the pharmaceutical, biotechnology and medical device industries. It specializes in the strategic development, management and analysis of programs that support clinical development – from compound selection to Phase I-IV clinical studies. The company operates from 98 locations in 38 countries and employs 13,250 people.

As a clinical research organization with a global footprint, ICON operates in a regulated industry in which it must adhere to strict FDA requirements, master service agreements and statements of work with customers. Due to the sensitive nature of its work, ICON takes security seriously. "Just like any other security organization, our websites are subject to attacks, users click on malicious links, and we worry about data loss. As a clinical research organization trying to get a drug to market, we have confidential information on drug trials that must be secured," explains Tony Clarke, Head of Information Security, ICON Plc.

Security In Highly Regulated Environment

To continually assess its security and provide metrics to management about the state of the company's security, ICON found itself performing a lot of penetration testing. However, to plan and execute this testing and address remediation annually was taking over 12 months. "We wanted the security assessment process to become faster and quicker," says Clarke. "Additionally, the success of manual penetration testing is dependent on the skillsets of the individuals performing it, which can vary."

ICON sought an automated way to validate the strength of its cybersecurity protections and understand where it needed to make improvements. It also wanted the ability to show auditors in a highly regulated environment where they were making improvements in security. Finally, the company is continually seeking new ways to demonstrate to customers its commitment to security.

ICON isn't alone in the security challenges it faces. Despite an ever-increasing number of technologies deployed, attackers are succeeding more than ever before. In fact, the third edition of the Hacker's Playbook™ Findings Report found that over 60 percent of malware infiltration attempts succeed, and lateral moves are successful nearly 70 percent of the time. In most cases, organizations are continually implementing security controls but without an effective way to validate that they are working as expected. Without an automated and consistent way to validate the efficacy of security products, security exposure from implementation, misconfiguration and non-optimized products can occur.

SafeBreach Delivers Value

ICON analyzed solutions in the Breach and Attack Simulation market. "We evaluated several vendors but they simulatedvery niche scenarios," says Clarke. "For example, one vendor simulated only browser attacks. We wanted simulations that could provide complete kill chain visibility: infiltration, lateral movement, exfiltration."

ICON found that SafeBreach, the leader in Breach and Attack Simulation, was able to deliver on the company's requirements. The SafeBreach platform provides an "attacker's view" of an enterprise's security posture to proactively predict attacks, validate security controls and improve SOC analyst response. Using simulators deployed across the environment, SafeBreach simulates thousands of attacker techniques from the Hacker's Playbook™ automatically, continuously, and safely, to prove where security is working and uncover areas where attacks will break through.

ICON evaluated SafeBreach in a proof of concept (POC) environment that quickly turned into a production deployment. "Security teams often don't have resources and bandwidth to properly test products to see what's actually working and what's not. We found SafeBreach provided a repeatable, well-implemented way to properly test our security capabilities," says Mick Ryan, Cybersecurity Operations Manager, ICON plc.

"The more we worked with SafeBreach, the more use cases we found," says Clarke. ICON used SafeBreach in a secure web gateway production rollout to test SSL and exfiltration capabilities. When ICON migrated from IDS to IPS deployments, it also used SafeBreach to validate prevention policies.

SafeBreach is helping in ways ICON didn't envision as well. "ICON is very active in mergers and acquisitions," says Ryan. "We deploy SafeBreach simulators into an M&A environment and look at the results, which is really helpful. In addition, we long suspected that one of the A/V products we use is better than the other, but with SafeBreach we actually had the data to prove it."

SafeBreach

Security Metrics From Simulations

SafeBreach has helped ICON achieve its goals and reduce its security exposure. "Every week we run the entire SafeBreach playbook to identify any security gaps in our environment," says Ryan. ICON's security team also uses SafeBreach to validate SOC alerts and responses. "SafeBreach is front and center within the SOC operations," says Ryan. "The first time we ran the simulations, we were alerted by the SOC team. After running them for a couple of months, we could see our team's response pattern. Our SOC team still reports on SafeBreach events and we can check their response times."

The ICON leadership team began receiving the metrics on security it desired. "We explored a number of options – from simulated phishing attacks, results of penetration testing, missing patches and more – and found SafeBreach provided the highly comprehensive metrics management needed about the state of our cybersecurity," says Clarke. "SafeBreach simulates infiltration, lateral movement and exfiltration methods and the playbook encapsulates all the major cybersecurity threats – by simulating data breach, data loss and malware threats, you're also assessing patching effectiveness, network segmentation, security monitoring and detection, and prevention controls."

ICON appreciates that using SafeBreach makes security testing more uniform and reliable. "Skilled penetration testers are hard to find and they will have constraints and time deadlines," says Clarke. "Breach and Attack Simulation is comprehensive, automated and continuous. SafeBreach has given us consistency and scale to test security controls in an intelligent way and improve our security."

SafeBreach

HQ

111 Evelyn Avenue #119

Sunnyvale, CA 94086

contact@safebreach.com

R&D

108 Igal Alon Street

4th floor Tel Aviv, 6789146

ISRAEL