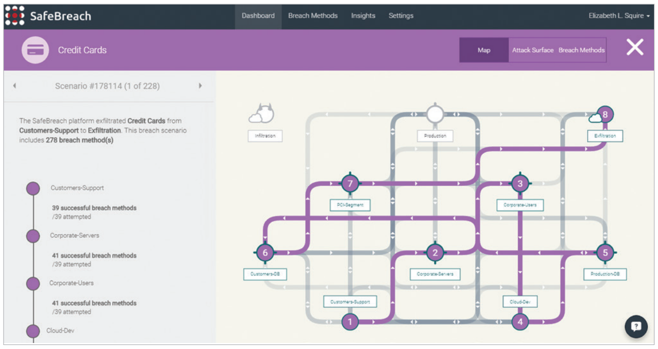
SC MAGAZINE First Look



Scenario #178114 (1 of 228)

The SafeBreach platform exfiltrated **Credit Cards** from **Customers-Support** to **Exfiltration**. This breach scenario includes **278 breach method(s)**

Customers-Support

39 successful breach methods
/39 attempted

Corporate-Servers

41 successful breach methods
/39 attempted

Corporate-Users

41 successful breach methods
/39 attempted

Cloud-Dev

SafeBreach

Continuous Security Validation Platform

If you like really innovative – and useful – cyber defense tools, you will love SafeBreach. We read the background information on this one and, frankly, our first question to the company was: "How is this not just a fancy penetration testing tool?" As it turned out, the answer came very quickly; in fact, within moments of turning the tool on. And the answer? The two types of tools don't even play in the same ball park.

The whole idea behind SafeBreach is that it provides an attacker's view of the enterprise. A major issue in pen testing is exploitability. It's one thing to have a report full of vulnerabilities, but if they cannot be exploited the risk is lower. The problem is that exploitability – once the province of human hackers – now is even more the province of malware or, more commonly, malware in combination with humans.

By using their "Hacker's Playbook," SafeBreach is able to develop breach scenarios unique to your environment and then run simulations. By correcting problems the tool finds and re-running, you iteratively secure your enterprise far beyond simple pen testing for continuous improvement. It's no secret that attackers are evolving constantly – your enterprise defenses need to also.

SafeBreach Continuous Security Validation Platform consists of two parts: the Orchestrator (cloud) and Breach Simulators (on-premises). Together they try to answer the question: "How safe am I?" When you start up the tool, you drop into the dashboard. This is broken down into Critical Services Breached, Infiltration and Data Assets Exfiltrated. Immediately you're playing on a real-world playing field.

Setting the tool up is simplicity itself. All you need is the IP of the management server and the Continuous Security Validation Platform does the rest. Even though there are lots of scenarios provided, you can finetune them for even more customization within your enterprise. The tool integrates with Splunk, so if you're a Splunk shop you have even more power available. As you remediate, you continue to run scenarios – taking into account that there are new ones weekly to keep up with the bad guys.

There are lots of different views of the overall process. One we especially liked was Insights. This is a graphical view of what assets and services are most at risk. Think of a heat map with an attack surface on the vertical and a number of locations on the horizontal. It's hottest in the upper right-hand corner where the attack surface is the greatest, and the number of locations is as well. That quadrant is not where you want to be. You want to move as many assets and services to the lower left corner as you can. This is a presentation that is useful from a practical standpoint and easy to understand and explain to non-technical management.

Overall, we enjoyed working with this one. Pricing is very flexible depending on what you want in your package, and support is right where it needs to be.

– Peter Stephenson, technology editor

AT A GLANCE

Product Continuous Security Validation Platform

Company SafeBreach

Price Depends on number of simulators deployed.

What it does Simulates and validates breaches so that security teams can architect defenses more effectively and recover from events more rapidly.

What we liked The whole idea of simulating all possible breaches in a given environment.

The bottom line This is a very cool product and it definitely is not your typical pen testing tool. Characterizing SafeBreach in that manner is a bit like saying the *QE2* is a boat.

SafeBreach

SafeBreach
111 W. Evelyn Avenue, Suite 119
Sunnyvale, CA 94086
www.safebreach.com/

Reprinted from the March 2016 issue of SC Magazine • www.scmagazine.com