ceocfointerviews.com

Issue: February 29, 2016
The Most Powerful Name in Corporate News

Cloud-Based Security Safety Validation Platform that Continuously Mimics and Tests for Data Breaches within the Entire Network of an Organization

Stephan Chenette
Co-Founder & CEO
AttackIQ, Inc.

CEOCFO: ***Mr. Chenette, what is AttackIQ?***
Mr. Chenette: AttackIQ is the first company to provide a continuous security testing platform that challenges existing network and cloud infrastructure. Its flagship platform, FireDrill™, helps organizations safely validate the assumptions about their own defense in depth strategy, no matter where they are in their security life cycle. By duplicating real-world attacks and safely applying test scenarios in active environments, FireDrill provides security assurance to validate if deployed solutions are providing protection as designed. Headquartered in San Diego, California, AttackIQ's management team has more than 20 years of experience leading security teams at some of the world's top security companies.

CEOCFO: ***How are you able to help a company that has made the assumption they are doing all of the right things and wakes up one day and realizes that might not be the case?***
Mr. Chenette: First we help them by providing a scenario that can be deployed into their infrastructure to test each assumption they have about their own security program. Our FireDrill platform can run these scenarios on an ongoing basis so that even when the IT staff of a company has gone home for the day, the platform is continuously and automatically running the scenario at the discretion of the IT Staff who can say when, where and how these scenarios should be testing. If this is the first time they have tested their assumption, in many cases their assumption will be wrong. In that case, what our technology provides is not only the capability to test their assumption but simple prescriptions that provide a mitigation strategy to help minimize risk.

CEOCFO: ***How does it work?***
Mr. Chenette: The FireDrill platform is cloud-based or on premises, you sign up, deploy software agents throughout your on-premises and cloud network, run scenarios and view results. We have thousands of scenario categories to choose from. Our core focus is on validation and attack scenarios. This can range from security technology categories such as advanced end points, web filtering and firewalls to attacker techniques, personas and recent data breaches such as the Target breach. We also have scenarios that can be integrated to make use of threat intelligence feeds the organization is already receiving. We want our customers to be able to challenge their existing infrastructure and utilize our scenario library to do so.

CEOCFO: ***Is it up to your client to pick a scenario or put together a scenario with your tools or do you guide clients in some way?***
Mr. Chenette: Our customers have absolute control in what scenarios to run, where it's run and how often it's run. We offer videos and tutorials as well as white papers to help guide them through our scenario and mitigation library so that they can get the answers to their questions or test their assumptions. If our customers need expertise, we provide guidance through our customer support channels, services team and partnerships.

CEOCFO: ***New viruses come out every day. Is there a timeline that people should be testing?***
Mr. Chenette: The networks of enterprises large, medium and small are changing every day. There are new employees, new technologies, new changes to the network, so because the network is changing continuously you should be testing the network continuously. For some organizations that might be every hour. For others that might mean a few times a day and for others it might mean testing the network every time there is a change. We want to give the power to the IT and

security teams to determine when they should be testing and allow them to be able to test with a platform that can provide consistent, repeatable testing.

CEOCFO: ***Are similar systems available? Has this approach been thought of or used before?***
Mr. Chenette: The idea of understanding your own network from the viewpoint of an attacker is key to being a good defender and truly understanding your risk. However, up until this point there has not been a platform available to help you in continuously validating your security infrastructure through the same eyes as an attacker. The only options have been hiring consulting firms which is costly and only offers a point-in-time assessment. The AttackIQ FireDrill platform allows an organization to validate their own defense-in-depth strategy at minimal cost, time and resources.

CEOCFO: ***There are so many approaches to security. How have you been able to develop the FireDrill so that it hits every end of where an attack could be?***
Mr. Chenette: Cyber security is a business issue, not an IT issue. Organizations have to have an understanding of their business assets, the value of those assets and what mechanisms they have in place protecting those assets. Validating your security infrastructure is a systematic approach that can be done in two ways: 1) by looking at your assumptions of the protection mechanisms in place and unit testing those assumptions and 2) by taking an entire attack chain that your organization is concerned with and testing them against your entire holistic security defense-in-depth strategy. Both methods will help you to identify blind spots and incorrect assumptions. In the end it will minimize your risk.

"FireDrill enables organizations to create a baseline for security and to help them make better data driven decisions to spend budget wisely and in the end lower their risk of a data breach. It is very important for organizations to stop assuming and start knowing."- Stephan Chenette

CEOCFO: ***How long has FireDrill been available?***
Mr. Chenette: After two years of working with strategic customers, we released FireDrill into general availability January 20, 2016. By visiting our website at https://attackiq, we offer qualified companies a two week free trial to test their own security infrastructure.

CEOCFO: ***How are you getting the word out about AttackIQ?***
Mr. Chenette: In the last two and a half years AttackIQ has been working with a number of the Fortune 100 and Fortune 500 companies. Early on we selectively worked with companies that lead the path for early adoption of key technology. We have been gaining a lot of traction through our early adopters that have seen the value our platform has brought them and has shared that value with their own verticals. Now that we are out of stealth you can expect to see us speaking and hosting events at industry conferences. For example, we will be speaking at RSA this year on how to minimize risk through continuous security control validation. We do feel we are providing a true disruptive technology to the Cyber security industry. It is a new area that companies will have to start paying attention to or be left behind. Instead of buying the "next generation" security product that promises you that it is in fact the silver bullet of detection, they should start testing their own current security investments to truly increase the return on investment (ROI) of current investments and understand future investments.

CEOCFO: ***Are people skeptical?***
Mr. Chenette: People aren't skeptical. Once they read about AttackIQ and they think about the model of "trust, but validate", they get a moment of obvious realization, wondering how they never thought that they could validate their own assumptions and they had to continue thinking hope was a strategy. We have provided a platform that we want the community involved in, so anyone can write scenarios for the FireDrill platform, in doing so, we can move from simply a discussion of uncertainly to true risk quantification.

CEOCFO: ***Where are companies often vulnerable that they just might not even think of as a problem?***
Mr. Chenette: Every company is vulnerable. What matters is that they take steps to minimize the impact of a threat. In order to understand the impact of the threat, safely running scenarios that allow an organization to find weaknesses and improve on those weaknesses over all minimizes risk.

CEOCFO: ***Are you able to discern what looks like a real attack, but might not be?***
Mr. Chenette: The FireDrill platform will help test your products, processes and technologies, so that your incident response team is better prepared to prioritize events. Your security operations team understands the capabilities of it's own technology better and the so that your entire team is better prepared for an attack and is able to minimize the risk of that attack truly having an impact on the business.

Imagine the power for a CSO to say, “In the last quarter we increased our response time by X percentage,” or “We increased our detection rate by ten percent.” With FireDrill you can essentially run a series of scenarios and measure and quantify your current security posture and in a month or in a quarter, understand how your baseline increased or decreased.

CEOCFO: ***Can you envision a time perhaps when insurance companies would require FireDrill?***
Mr. Chenette: Cyber insurance is currently in its infancy. Under writers are having a difficult time pricing premiums. It will become more and more a factor to quantify the security program of an organization. As Cyber insurance becomes something every company starts to purchase, having a platform like FireDrill that can help minimize risk, and quantify the resiliency of your network will help drive down the premiums for organizations in the cost of buying Cyber insurance.

CEOCFO: ***What about the government market?***
Mr. Chenette: The government systems and networks need a platform like FireDrill. Let’s take the recent Office of Personal and Management (OPC) breach as an example. It’s crucial that organizations that are responsible for such critical data validate their own security measures. In the case of OPM, it was shown that the organization simply did not have the security measures in place that the public assumed they did.

CEOCFO: ***Are you funded for the next steps that you would like to take for the rollout?***
Mr. Chenette: Yes. AttackIQ is funded and will be growing substantially this year.

CEOCFO: ***Why are AttackIQ and FireDrill so important today?***
Mr. Chenette: AttackIQ and FireDrill are important because if you cannot measure your security posture you cannot improve it. Today we lack true metrics in security. FireDrill enables organizations to create a baseline for security and to help them make better data driven decisions to spend budget wisely and in the end lower their risk of a data breach. It is very important for organizations to stop assuming and start knowing.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

AttackIQ, Inc.

For more information visit:
www.attackiq.com

Contact:
Stephan Chenette
+1 415 413 7353
info@attackiq.com