WHY A 24/7 FULLY AUTOMATED BREACH AND ATTACK SIMULATION PLATFORM IS NEEDED TO SECURE YOUR ORGANIZATION'S CRITICAL ASSETS

By Chris Foster, Director of Field Engineering, XM Cyber

Global spending on information security now exceeds $100 billion annually, according to Forbes Magazine.

Unfortunately, organizations aren't getting a great return on their (quite sizable) investments. New, high profile data breaches seem to occur on a near-constant basis, and losses from cyber-attacks have never been larger. It's estimated that security breaches will result in a staggering $6 trillion in annual losses by 2021.

To cope with unceasing pressure from bad actors, many organizations adopt a posture of "more is better." They spend more money — and add more layers of security — and hope for the best.

This is a long-term recipe for failure, however. To provide the best possible defense, organizations need to rethink how they approach information security, and how they evaluate the products they deploy. Ultimately, if you want objective evidence of the strength of your defenses, it all comes down to testing. Yet conventional testing methods, too, suffer from their own innate weaknesses.

Let's take a closer look at the efficacy of some conventional testing methods, and then explore why a fully automated breach and attack simulation (BAS) solution offers a novel and highly effective approach to testing and security.

PENETRATION TESTS

Penetration testing has long been considered one of the most effective mechanisms for evaluating organizational defenses, as it helps establish the strength of perimeter defenses. A penetration test will identify, rank and rate vulnerabilities and offer remediation assistance.

Yet penetration tests have drawbacks. If done improperly, they can damage organizational assets. Test results may be misleading if conditions are not realistic. Most importantly, penetration testing is typically episodic, which means security teams have little insight into the state of their defenses when tests are not being performed. Security teams also must wait until the next scheduled test (which may be weeks or months away) in order to gauge the effect of changes in an enterprise environment.

RED TEAM TESTING

Originally developed by military researchers, red team tests are very effective at mimicking advanced persistent threats that can embed themselves in a network for weeks or months. These threats can then move laterally and steal an organization's crown jewels. During red team exercises, ethical hackers attack a digital infrastructure by simulating the kind of attacks most likely to be launched by black hats.

While red teams are highly skilled at simulating sophisticated attacks, these tests are resource-intensive. Because of this — and because they are led by humans — continuous red team testing is not an option for many enterprises.

VULNERABILITY MANAGEMENT TOOLS

These scans are helpful tools for detecting commonly known vulnerabilities and monitoring patching, yet they have a somewhat limited effect. Most do not allow a security team to ascertain the potential impact of identified vulnerabilities, nor do they incorporate checks for defensive measures designed to inhibit lateral movement by attackers. While useful, such limitations can fail to illuminate threat activity from sophisticated adversaries.

VULNERABILITY MANAGEMENT TOOLS

These scans are helpful tools for detecting commonly known vulnerabilities and monitoring patching, yet they have a somewhat limited effect. Most do not allow a security team to ascertain the potential impact of identified vulnerabilities, nor do they incorporate checks for defensive measures designed to inhibit lateral movement by attackers. While useful, such limitations can fail to illuminate threat activity from sophisticated adversaries.

> *“An automated, continuous solution helps organizations take an entirely new approach to evaluating security. As Gartner noted: “Penetration testing helps answer the question ‘can they get in?’; BAS tools answer the question ‘does my security work?'” Likewise, XM Cyber is the only one to address the most crucial question for enterprises: ’Are my crown jewels really secure?’”*

THE BOTTOM LINE

Ultimately, all these testing approaches suffer from the same critical drawback: They do not offer continuous and comprehensive feedback regarding an organization’s holistic security posture. They can offer insight into the state of organizational security, but these insights are snapshots from a moment in time and do not illuminate all the potential attack paths to key critical assets. For more robust security, organizations need more than a snapshot: They need the information security equivalent of a security camera running 24/7, 365 days each year.

And that’s the promise offered by today’s BAS solutions.

THE VALUE PROVIDED BY AN AUTOMATED BREACH SIMULATION

A BAS platform operates in a similar fashion to red teaming. This technology simulates complex attacks and tests organizational defenses against such attacks. These platforms can simulate phishing attacks, malware attacks on endpoints, data exfiltration and sophisticated advanced persistent threats employing lateral movement.

Because the technology is fairly new, BAS solutions can differ considerably in features, functionality and deployment options. Yet they all have one key differentiator with regard to conventional testing methods: Automated breach simulations aren’t run episodically. They can run around the clock and provide continuous testing and improvement, ensuring that organizations have full visibility into the state of their security. No more long gaps necessitated by the expensive and time-consuming nature of more manual testing methodologies.

Additionally, continuous testing is an even greater imperative given the state of most enterprise security environments. According to Gartner, most large enterprises have between 30 and 70 security vendors. As vendors update their solutions, continuous testing is necessary to ensure that these changes do not create new problems within the overall defense landscape. When enterprises are piling products on top of products — and those products are introducing a steady stream of changes — new security issues are bound to arise.

An automated, continuous solution helps organizations take an entirely new approach to evaluating security. As Gartner noted: “Penetration testing helps answer the question ‘can they get in?’; BAS tools answer the question ‘does my security work?'” Likewise, XM Cyber is the only one to address the most crucial question for enterprises: “Are my crown jewels really secure?”

Given that today’s organizations are under siege from threat actors, these are questions of paramount importance.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber’s core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker’s techniques and methods.

CHRIS FOSTER

Chris Foster is the Director of Field Engineering at XM Cyber. He has over 17 years of security experience serving both public and private sector organizations. He previously held senior security positions with Flashpoint, iSIGHT Partners, FireEye and Chevron. Chris spent over a decade in the public sector at numerous organizations, including Booz Allen Hamilton and SAIC, supporting various U.S. Military and Intelligence Community. degree from Vanderbilt University.