XM CYBER

A CLOSER LOOK AT CYBER ATTACK SIMULATION

By XM Cyber Team

Cyberattacks are growing steadily in number, strength and variety, but in many cases the efforts required to combat them are still crawling. Top-notch hackers can mimic legitimate user actions and go under the radar of protective measures. They can move laterally from hole to hole and reach what matters most to you – your crown jewels.

What if you could see your organization through the eyes of the attacker? The good news is that there are tools that can simulate cyberattacks and help you win this battle. Simulation is truly a game changer. It runs exhaustive scenarios, which are safely activated simultaneously and continuously within the production environment, exposing attack vectors and compromised assets.

The result of cyberattack simulation is that you can check every possible route and type of attack vector – from the attacker's perspective – to see where the organization is at risk and take actions to remediate. The best part is that some cyberattack simulation tools allow you to automate the action.

Many CISOs still consider zero-day threats one of their chief concerns. Yet they are actually being employed much less frequently and most cyberattacks are surprisingly unsophisticated – so simple, in fact, that the National Security Agency (NSA) reports 93% of them could be prevented just by incorporating some basic best practices.

It turns out the hackers no longer need to put in the time-consuming effort necessary to construct elaborate new attacks, because they know they can sneak through companies' defenses just by taking advantage of poor IT hygiene.

PENETRATION TESTING AND RED TEAM ASSESSMENT

A penetration test detects and exploits vulnerabilities throughout your network and infrastructure. During a pentest, specialists use real-world attack techniques to achieve a predefined objective on the target environment. Although the technique has been widely used for several decades, there are other market solutions that organizations can use to test their security.

A red team gives the organization the opportunity to test its security team against the techniques and approaches used during real breaches, see how the team reacts, and identify points of improvement. Therefore, red teams have been gradually introduced by many organizations.

Pentesting can overlap with red team exercises and this may be a bit confusing to some people. It turns out that penetration testers and red teams are the same people, using different methods and techniques for different assessments. They are like judo and karate, or sumo and krav maga – one is not necessarily better than the other and organizations see value in both. When combined, they can present a company with a good, point in time, risk evaluation.

THE EVOLUTION TO BREACH AND ATTACK SIMULATION (BAS)

Recently, a new category of solutions has emerged to help with this problem. Breach and Attack Simulation (BAS) tools allow organizations to continually and consistently simulate the full attack cycle against their infrastructure, using software agents, virtual machines, and other means.

BAS automates the testing process and performs it continuously. While these tools may not have the same creativity and ingenuity as human white hats, they can test all the time across a broad spectrum of attacks.

BAS products are becoming more mainstream and have begun transforming the security testing landscape. “The tools we looked at all used simulations to test network security in a risk-free environment. While this may limit what they are capable of simulating, these tools provide a lot of insight on security holes and can greatly decrease the manual effort required during testing,” wrote SC Magazine.

PURPLE TEAM: SIMULATE AND REMEDIATE

Many red and blue teams (the company’s own IT personnel who defend their organizations around the clock) have worked very much in silos. In some cases, these teams can get out of sync. A purple team should enhance red and blue teams’ existing capabilities and allow them to exchange ideas, observations and insights more productively.

All three forces share the ultimate purpose of improving the organization’s defenses. Red does this through “ethical attack,” blue through defense, and purple by ensuring that the previous two are cooperating.

With an automated purple team running continuously, organizations will finally be able to follow prioritized remediation guidelines and know as soon as an issue has been resolved. The move to automation empowers organizations with the ability to gain a worm’s eye view into new back doors and blind spots as soon as they appear and move to remediate them immediately without delay.

Automated BAS continuously exposes attack vectors, from breach point to any organizational critical asset. This continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of security gaps.

In effect, a quality BAS solution operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of the hacker.

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.

XM CYBER® TEAM

XM CYBER TEAM

The XM Cyber team consists of the best cyber security specialists in the world. Their thought leadership helps inform and educate customers globally via webinars, videos, articles, books and industry presentations. Join us online at xmcyber.com for more in-depth analysis and recommendations on cyber security best practices.