AN INTERVIEW WITH MENACHEM SHAFRAN
VP PRODUCT, XM CYBER

SUPPORTING BREACH AND ATTACK SIMULATION

THE process of breach and attack simulation is clearly one of the important new controls in cyber security. Benefits include validation of controls over a continuous period, and exercise of attacks from the best available taxonomies of known (and unknown) methods. The result is that most enterprise teams now utilize some form of simulation for this work, and excellent automated platforms are commercially available.

XM Cyber is an industry leader in this area of breach and attack simulation with a platform that effectively integrates with other aspects of an enterprise architecture. Led by veterans with military intelligence backgrounds, the company makes good use of attack frameworks and offers an excellent validation experience. We spent time with Menachem Shafran of XM Cyber who shared his insights into this important area of cyber security and how the company's platform is evolving.

EA How does attack and breach simulation work in the context of enterprise security?

MS Breach and attack simulation works in enterprises by continuously simulating attacks on the environments, in a safe way, without creating additional risks. With BAS tools, enterprises gain a measure of how effective their security is and where they should focus their efforts to improve it. The value measuring continuously allows enterprises to detect changes that create a risk in near real-time and to act upon them, greatly reducing the risks. In most cases, the security team will review the results every few days and update their workplan accordingly while also validating the impact of changes as they are made. This is a great improvement to just looking at vulnerabilities or performing manual red team exercises every few months.

EA Does simulation require buyers to conceive scenarios or does automation cover this action?

MS Different breach and attack simulation tools work in different ways, yet most would not require the user to conceive the exact scenario. At XM Cyber, we ask the buyers to define the goals, meaning the target critical assets that the simulation will try to reach. The details of how the simulation will reach the critical assets are completely automatic. The simulation will look to find the most probable attack vectors towards the assets. Using this information, we can now help prioritize remediation efforts based on the impact each finding has on reaching the critical assets. This allows organizations to focus on the most critical issues they have instead of just guessing what to work on.

EA How does the XM Cyber platform work? How does it automate the simulation process?

MS The XM Cyber platform works by installing lightweight sensors in the environments. The sensors then learn the network and run

the attack simulation in a safe and accurate manner. One of XM Cyber's unique values is the fact that the platform runs the simulations on the production environment and not on separate devices. This allows us to discover the most realistic attack vectors possible by combining vulnerabilities, IT hygiene and misconfigurations, and user activities just like a real attacker would. The simulation process is completely automatic. The platform has many attack techniques in its hacking engine, and just like a real attacker it selects the most fitting on each step of the attack vector.

EA Do you make use of any attack frameworks such as MITRE ATT&CK?

MS Yes. The XM Cyber platform is aligned to the MITRE ATT&CK framework and we show the relevant ATT&CK techniques on each step of the attack. We believe that the ATT&CK framework is a great learning tool to help security teams understand how adversaries work and an excellent way to create a common language in the industry.

EA Any near or long-term predictions about breach and attack simulation?

MS I believe that breach and attack simulation will grow rapidly as more and more organizations will start to realize they can now measure their security posture effectively. I think we will also see many collaborations between, or perhaps among, BAS vendors and other security vendors such as vulnerability management solutions and endpoint protection in order to better provide value to customers by allowing them to view a more holistic understanding of the current risks in the environment.