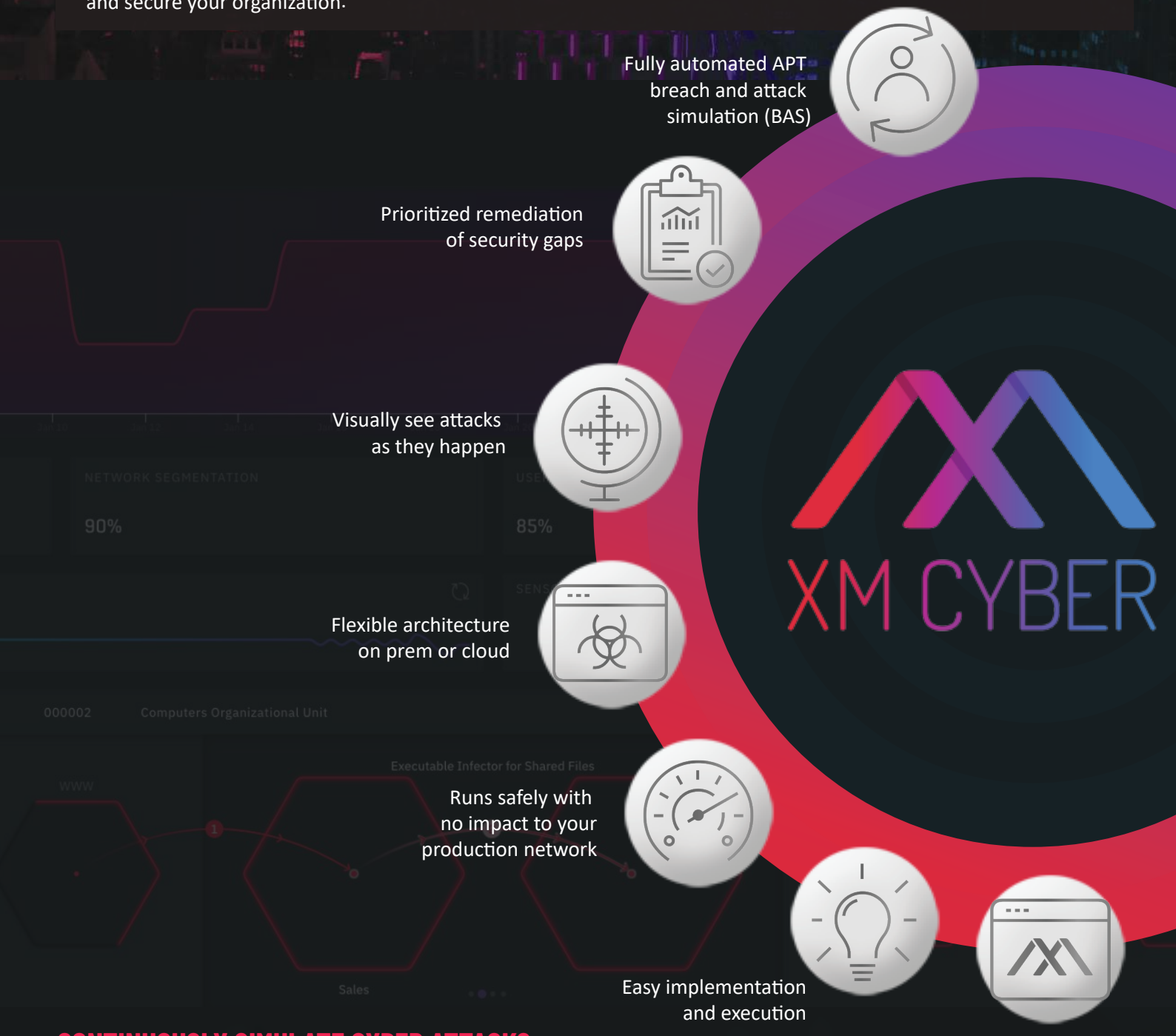
IT'S NOT ABOUT MORE SECURITY, IT'S ABOUT PROTECTING WHAT REALLY MATTERS

It's time to start thinking like a hacker.

View your network from their perspective. Watch for opportunities. Leverage employee activity. Combine multiple attack techniques into a single attack plan. Wait for a change to happen that exposes critical assets. All in real time.

XM Cyber puts you in the hacker's chair, giving you the latest tools and techniques to test your own environment. You select which assets are most critical. You launch an attack in your live environment and run it continuously, safely and 24/7.

You are rewarded with prioritized remediation recommendations to immediately correct and secure your organization.



CONTINUOUSLY SIMULATE CYBER ATTACKS THAT COULD THREATEN YOUR CRITICAL DATA

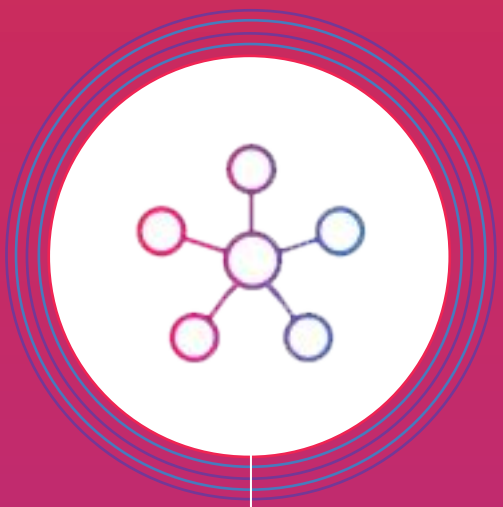
WHY

APT SIMULATION AND REMEDIATION

Manual testing is not effective because your network is constantly changing. To truly understand your risk, you need to run 24/7 in your production environment with tests that do not use active exploits.

Do you want to just test your security controls or understand all possible attack paths? That's the difference between an APT simulation and standard security control validation.

By identifying and prioritizing security that protects the most important data, XM Cyber customers optimize their existing security investments and significantly reduce risk and the impact of a breach.



Confirm any what-if analysis based on breach location and targeted digital assets

Use actual user behavior to identify real attack vectors

Improve overall IT hygiene and reduce misconfigurations and the effect of human error

Optimize your security staff and reduce dependence on manual testing

Prioritize security activities to protect your most important data

Automatically add the latest attack techniques to your defense strategy

XM CYBER

CASE STUDY

THE CONTROL VALIDATION PROBLEM

One of the largest banking organizations in the world relied on security control validation products. And yet, they were hacked. Now they understand that just validating that security tools are in place and working correctly does not protect that network from mistakes.

In this case, a hacker mimicked an employee to move in the open across security controls, taking advantage of poor IT hygiene and common errors in human judgement. XM Cyber now tests these attack paths continuously.

ABOUT

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.

Tel Aviv +972 3 978 6668 New York +1 866 598 6170 Sydney +61 2 8880 0705 London +44 203 322 3031 info@xmcyber.com