STOP ATTACKS BEFORE THEY HAPPEN
SEE YOUR NETWORK THROUGH THE EYES OF A HACKER

A dedicated hacker is going to evaluate your security measures and find ways around them. The question is what happens after they breach your perimeter.

XM Cyber gives you the ability to see your network the way the hacker sees it. It helps you to find all existing hidden vectors of attack, including those that typically go under the radar of most protective measures. And once an attack path is identified, XM Cyber delivers a focused and prioritized remediation report so you can fix those weaknesses before the hacker strikes.

Our patented approach helps you reduce your risk by exposing gaps resulting from unpatched systems, misconfigurations, software flaws and human error.

Regardless of your security controls, if there exists an attack vector that through any means can reach your critical assets, XM Cyber will find it.

XM Cyber is the only available solution that safely simulates an advanced persistent threat (APT) against your organization's critical assets.

More than a breach and attack simulation – a fully automated APT

Identify every attack vector that hackers can exploit

Protect critical data stored in AWS

Flexible architecture on prem or cloud

Runs safely with no impact to your production network

Prioritized remediation of security gaps

Validate your security controls

CLICK HERE TO GO TO https://youtu.be/G7SINpADHBY

SEE HOW XM CYBER CONTINUOUSLY EXPOSES ATTACK VECTORS THREATENING YOUR CRITICAL ASSETS AND PROVIDES YOU WITH PRIORITIZED, ACTIONABLE REMEDIATION.

FIND GAPS NO ONE ELSE SEES

EXCEPT THE HACKERS

Hackers explore every opening, waiting for changes that get them closer to your critical assets. The best defense is to take the same approach – be proactive in searching for attack paths.

Manual testing is not effective enough because your network is constantly changing. To truly understand your risk, you need to run 24/7 in your production environment, constantly improving your security posture.

Testing security controls is important, but you must also be able to detect all attack paths that evade your existing security products. And be able to see that attack as it travels across your entire organization, including your presence in the cloud.

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.

THINK LIKE A HACKER TO STOP A HACKER

Confirm no attack vectors allow access to critical assets

Automate combined red and blue team processes into an automated purple team

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

USE CASES

Cloud Migration Challenges. A financial institution was migrating core applications to the cloud. XM Cyber quickly identified that rules from the old environment were still in place. New devices were being added without protection. And multiple attack paths were exposed

IT Hygiene Issues. A network manager was in a hurry. He changed the admin rights on a server in order to update a new network wireless connection, forgetting to change them back. XM Cyber used those credentials to reach their financial server during a simulation.

Critical Infrastructure. XM Cyber regularly finds standard IT networks implemented in operational networks with links between the two systems. Even if hackers and malware cannot affect these operational systems, they can block access and effectively shut down entire operations.

Air Gapped Connections. Even air-gapped networks are susceptible to mistakes. XM Cyber has found both USB usage and improperly connected network connections that led to isolated networks allowing attack vectors.

Third-Party Connections. Suppliers commonly have access to their customer's network to simplify the supply chain. Credentials can be stolen from multiple points across the supplier and customer portals. XM Cyber continuously tests if those credentials and connections can reach your critical assets.

Purple Team Creation. A leading insurance company could not synchronize the efforts of their red and blue teams. Using XM Cyber, the customer unified the two teams, improving productivity by enabling a faster exchange of ideas, observations and insights. The result was greater visibility of the attack surface within their organization.

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.

XM CYBER

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