Complex, constantly changing digital networks represent an ongoing risk to most organizations. Information technology and cyber security teams are overwhelmed with alerts, software updates and new vulnerabilities. The only solution is to automate and integrate the right information at the right time to give clear direction across management, security and operations on where to focus. The end goal is to reduce risk associated with the most critical assets and optimize investments in capital and operating expense.

Not all vulnerabilities are created equal. XM Cyber combines advanced vulnerability scanning and patch management capabilities with its patented attack simulation engine to expose and remediate the greatest risks to your digital world. By adding additional context of how a particular vulnerability can be leveraged to compromise your critical assets, XM Cyber maximizes the effectiveness of your team’s ability to proactively secure what matters most.

The Challenges of Finding and Fixing

Identifying and remediating vulnerabilities is a constant problem. To stay ahead of attackers, your cybersecurity program must become an ongoing process that relies on automation and intelligent analysis to support your security and IT responsiveness.

The first step is to continuously scan your network for potential risk. Typically, security teams scan for vulnerability data and then request the IT teams update or patch the affected systems. Sounds easy but in larger organizations, this can represent hundreds or thousands of common vulnerabilities and exposures (CVEs). Each one must be researched and prioritized. In some cases, the issue is low risk or only impacts a minimal number of low-risk systems. Sometimes the fix is a patch that has been superseded by another patch. The IT team has no means of prioritizing.

The Difference Between Risk On and Risk To Your Critical Assets

Your vulnerabilities represent risks associated with a particular asset. What’s more important however, is identifying vulnerabilities that allow attack paths that lead to your critical assets. By prioritizing based on risks to versus risks on, you and your teams can pinpoint exactly the remedial activities required to close the complete attack chain related to your most critical assets. Ultimately, you lower or even eliminate risk while optimizing your team’s time and effort.
Let XM Cyber Enhanced Vulnerability Management Solve These Key Challenges:

**There are too many vulnerabilities to manage and patch.** By combining data from the VM module with XM Cyber’s attack simulation, you exactly the highest priority vulnerabilities based on their actual impact to your company, making sure your critical assets are patched. By focusing on the most critical patches, operations can reduce their immediate workload by as much as 90 percent because they only must focus on the 10 percent of CVEs that matter most.

**How do I bridge the gap between security and operations?** We know there is a big gap between what security is finding from vulnerabilities and what the IT or operations team is asked to do to fix those vulnerabilities. Looking up solutions to vulnerabilities is burdensome on operations. XM Cyber not only identifies not only the most important areas to remediate, but also provides you with information on the relevant and most recent patches, and where to deploy them.

**There’s too many scans and noise on the network from security tools.** Our lightweight sensor gives you full vulnerability assessment and attack simulation with very low impact to the performance of your endpoints.

**It’s difficult to understand the risks affecting the network.** XM Cyber not only gives you the most current list of vulnerabilities affecting your environment, including all the latest vulnerabilities, but it also analyzes misconfigurations and human error to understand all possible open pathways towards your critical assets.

**There’s too much data to analyze.** XM Cyber helps you and your teams easily understand the connection between a vulnerability, the devices it affects and the patches that can fix it to understand the scope of the problem and how to remediate it across your organization.

**I can’t assign tasks to various teams.** XM Cyber gives you the option to create a request for specific patches or devices and pass it to your teammates, executives or IT teams to act on it, with ability to keep and track the outbound requests to make sure nothing is missed or forgotten.
Key Benefits of XM Cyber Attack-Based Vulnerability Management

- Attacker-based vulnerability management solutions are the next generation of risk quantification for cloud and on-premise environments.

- As part of its remedial action process, XM Cyber points security and IT teams to the most accurate patch or update from the vendor saving hours and hours of research time.

- XM Cyber provides concrete evidence to the security and IT teams to justify the request for updating or patching systems and applications where business owners or others with authority and responsibility might resist due to unknown consequences or downtime required to accomplish the task.

Achieve Continuous Vulnerability Management

Our security solutions streamline the process from identifying, classifying, and addressing vulnerabilities to avoid threat actors exploiting gaps in time between security vulnerability reports and remediation. IT teams can easily import vulnerability scan results taken by Security teams. Quickly view the identified CVEs and associated patches and publish or approve any missing patches for deployment and save significant time.

You’ll improve the experience and productivity of IT teams that previously spent many hours researching, deduplicating, and preparing a patch group of updates manually.

XM Cyber is the global leader in Attack-Centric Exposure Prioritization, which is also known as Risk-Based Vulnerability Management (RBVM). The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities.

XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. XM Cyber helps to eliminate 99% of the risk by allowing IT and Security Operations to focus on the 1% of the exposures before they get exploited to breach the organization’s “crown jewels” – its critical assets.

XM Cyber was founded by top executives from the Israeli cyber intelligence community and has offices in North America, Europe, and Israel.

Tel Aviv +972 3 978 6668 | New York +1 866 598 6170
London +44 203 323 3031 | Munich +49 163 6288041
info@xmcyber.com