Defenders Think Lists. Attackers Think Attack-Graphs.

Prioritize risk remediation and secure your business-critical assets with continuous attack simulation

XM CYBER

Get the Context You Need to Lower Your Risk and Close Unknown Gaps in Your Security

The XM Cyber Attack-Centric Exposure Prioritization Platform shows you what could happen in your current environment and how to stop it

Harden your security where it matters most by removing the risks directly affecting your important business-critical assets

Networks change constantly and that creates problems for IT and security operations. Gaps open exposing pathways that attackers can exploit. While enterprise security controls like firewalls, intrusion prevention, vulnerability management and endpoint tools attempt to secure your network, breaches are still possible. The last line of defense must include constant analysis of daily exposures caused by exploitable vulnerabilities, common configuration mistakes, mismanaged credentials and legitimate user activity that exposes systems to risk of attack.

Why are hackers still successful despite significant investments in security controls? Several factors make securing your network difficult, mostly because of overwhelming alerts, never-ending software updates and patches, and numerous vulnerability notifications. Those responsible for security must research and evaluate piles of data without context. Risk reduction is almost impossible.

XM Cyber solves this problem by focusing your security investments where they can make the most impact on risk to business-critical assets. XM continuously scans your network and identifies exposures from exploitable vulnerabilities, misconfigurations, poorly managed credentials and risky user activities – these are the attacker golden nuggets, the essentials elements required for lateral move. The XM Platform then continuously simulates attacks towards your business-critical assets looking for attack paths that can be exploited. The result is a selective list of exposures putting your business-critical assets at risk. Context-sensitive least-effort remediation advice allows SecOps and IT teams to quickly patch the exposures.

The patented platform continuously simulates known and unknown attack vectors, using a hacker mindset to demonstrate what could happen. By continuously identifying new exposures from misconfigurations, poorly managed credentials and exploitable vulnerabilities, the platform shows your IT and SecOps teams what needs to be remediated, what the risk is to the rest of the network, and what steps need to be taken to fix the problem. More importantly, the platform also prioritizes the remedial activities based on risk factors associated with your most important, business-critical systems and data.

Deploy the XM Cyber Attack-Centric Exposure Prioritization Platform for Risk Reduction

Through continuously running risk-free in your on-premises, cloud or hybrid production environment, the XM Cyber Platform exposes attack paths that go unnoticed by other security controls. The accompanying, detailed remediation advice directs your security and network teams and prioritizes their actions based on criticality of the assets, the associated attack vectors and choke points, and additional contextual data.

The risk-free platform delivers context to your cyber security remediation programs, allowing your security and IT operation teams to achieve higher security posture and operational efficiency. You can now eliminate 99% of the risk to your critical systems by focusing on 1% of the exposures that can be exploited.

The XM Cyber Platform works closely with your existing security controls to give your teams additional information vital to rapid response. It's more than just attack simulation. The platform secures your cloud, prioritizes remediation to vulnerabilities, identifies unknown and undiscovered attack paths, and demonstrably reduces risk.

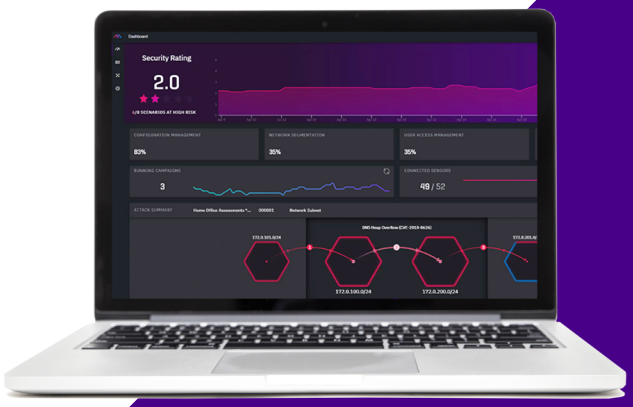
Breach and Attack Simulation

XM Cyber's Attack-Centric Exposure Prioritization is a new approach to Breach and Attack Simulation (BAS). Unlike other BAS vendors that check if security controls are properly configured, XM Cyber starts with identifying the most critical assets and identifies all attack path possibilities.

Then it quickly connects the dots from breach point to critical asset if there exists any potential attack path. Next, it creates a prioritized remediation plan, based on real risks to your critical assets, that directs your teams to quickly eliminate steps hackers would take inside your environment.

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.

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.

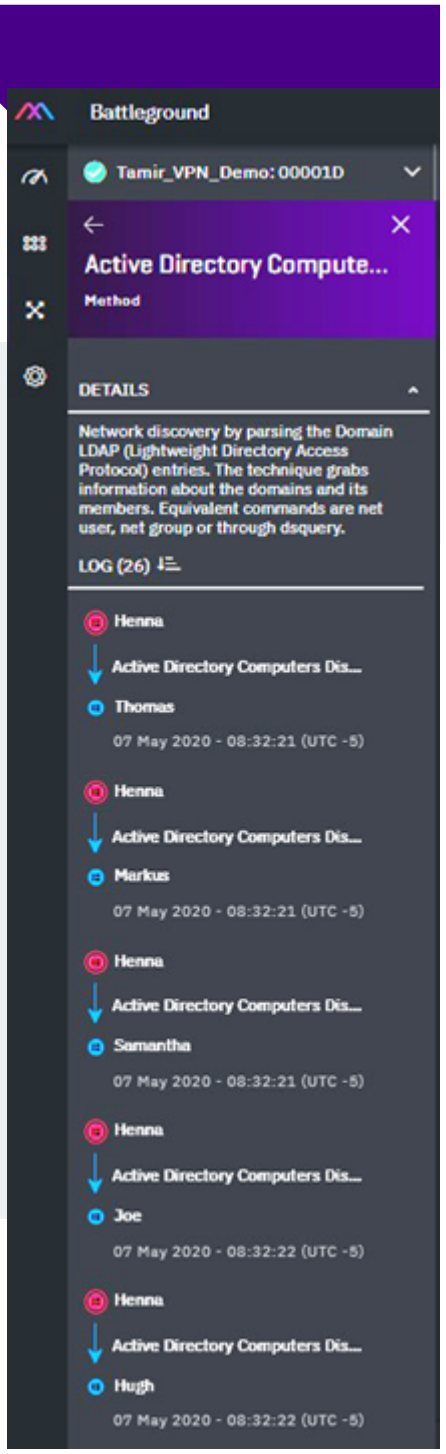


Key benefits of XM Cyber include:

- Run risk-free with no impact to your production environment
- risks as they arise by continuously looking for attack vectors
- Validate your remediation efforts and track your overall security posture and risk level
- Discover hard-to-find exposures that result from misconfigurations, vulnerabilities, misplaced credentials and poor user behavior
- See how attackers can pivot in your environment and use multiple vulnerabilities and exposures to form new attack vectors that lead to your business-sensitive assets

Attack-Based Vulnerability Management

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.



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
- New patches released by vendors often replace, or supersede, the previous patch release. XM Cyber solves this problem by always offering the right patch at the right time

Using attack simulation in conjunction with vulnerability scanning, XM Cyber delivers the next generation in vulnerability management. Now security and IT teams can work together, relying on additional context to evaluate the criticality of each vulnerability to prioritize and manage updates and patching. The benefit to customers is a continuous approach to vulnerability management that reduces risk while also reducing man hours and improving processes between security and operations.

Cloud Security Posture Management

Analyst firms like Gartner regularly report that most attacks happening in cloud-based environments are from error, not vulnerabilities. Most organizations are still in the early stages of adopting cloud services. Constant change and new ways of working can easily create gaps in your security, particularly when combined with a hybrid network environment.

Key Benefits of XM Cyber Cloud Security Posture Management

- Quickly identify security issues during migrations when changes are happening rapidly
- Find attack paths from on premise network devices that reach AWS assets
- Audit configurations via an API and calculate different attack vectors to find misconfigurations leading to risks such from unmanaged privilege escalations or access token theft

Add Context by Integrating with Your Security Ecosystem

You need to continuously identify exposures that cause risk

The goal of your security is not just to remediate incidents. XM Cyber helps prioritize work for your security and network teams that will have the most impact on reducing risk to your business-critical systems. By adding context to alerts and notifications from your existing security controls, XM Cyber helps your teams understand the potential impact, criticality of each asset, and related connections and choke points so they can prioritize their actions.

Security Orchestration, Automation and Response

The next step in your SOAR strategy should be to build an attack-centric exposure approach to evaluating all the information at hand. More importantly, the additional information should reflect your actual environment, and therefore, it also prioritizes remedial actions based your true risk potential. Relying on outside industry statistics for risk can be helpful, but not accurate. A small-risk incident report might go unresolved when in fact in can be a steppingstone to your crown jewels. It's all in the context and that's what your security teams need to have at their fingertips.

Cloud and Hybrid Environments

As more and more data are migrated to the cloud, new risks emerge making it critical for companies to assess their risk posture and understand how attackers can operate within their cloud environment. XM Cyber closes the loop between on-prem and cloud risk assessment via its patented, automated Attack-Centric Exposure Prioritization (ACEP) platform.

Endpoint Detection and Response

Your analysts need more information about assets where your endpoint detection has identified an issue. When alerts are received that a specific asset is at high risk, your security analyst can rely on XM Cyber to provide additional information on the criticality of that asset, what impact its compromise has on other assets in the network, as well as how to fix it.

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 +44 203 322 3031 | Munich +49 163 6288041
info@xmcyber.com

XM CYBER