Use Case

XM Cyber | See All Ways™

XM Cyber for Breach and Attack Simulation

Add context to your security strategy with Attack Path Management

Cyber security teams continue to be challenged by too many alerts, incident reports, vulnerability notices and a growing list to potential attackers. Standard security controls must be put in place and kept up to date. However, gaps still form constantly because of exploitable vulnerabilities and exposures from unmanaged activities like misconfigurations, mismanaged credentials, and risky user activities. Attackers can combine known vulnerabilities with these additional exposures across your network to move in and around your enterprise looking for critical assets.

The only answer is to continuously calculate all attack paths using simulated attacker techniques. Using the resulting data gives your security and network teams the attackers perspective into risks, regardless of other security scores or vulnerability notices. Now they can optimize their time and resources by prioritizing remedial actions based on real threats to business-critical assets in your actual environment.

By following an attack-centric, riskprioritization approach, you can eliminate 99% of your security risks by focusing on the 1% that represents the greatest risk.

Next Generation of Breach and Attack Simulation

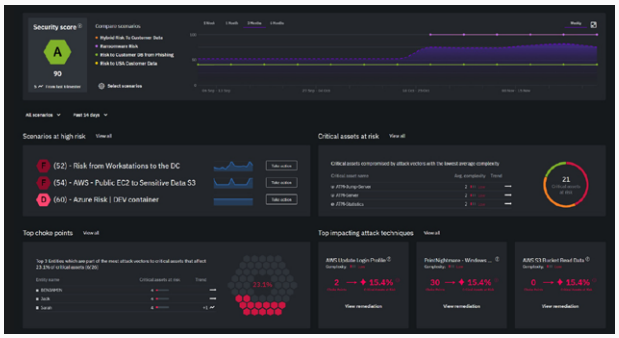
XXM Cyber's Attack Path Management platform is a step beyond traditional Breach and Attack Simulation (BAS) solutions. Unlike other BAS vendors that check if security controls are properly configured, XM Cyber starts with identifying the most critical assets and identifies all attack path possibilities.

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.

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.

Now you can truly see your cyber risk and proactively act to eliminate risk.



Go beyond Typical BAS with Context-Sensitive Remediation Advice

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.

Key Benefits

- Run risk-free with no impact to your production environment.
- Discover 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 assetsresponses and optimize resources

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.

See Attack Paths and Drill Down to Discover the Details

At the core of XM Cyber is the visual battleground that automatically generates a network map and displays assets and the chronological flow of possible attack paths within your live environment. Your security teams can drill down for asset discovery or to identify the exact technique used by the virtual hacker to move from one step to the other.

For instance, you can visually see how an attacker could exploit a vulnerability, proceed to harvesting strong cached credentials, pivot to your cloud account and leverage IAM privilege escalations to reach your critical assets.

The field-proven platform is simply and rapidly deployed in three simple steps, beginning with the selection of targeted assets, activation of ongoing attack scenarios and generation of prioritized actionable remediation, all in a continuous loop.

Integrate and Add Context to Endpoint and Vulnerability Tools

XM Cyber optimizes and protects your investment in security by assuring so additional attack paths can bypass or evade those controls. Your teams also gain risk-based additional context to help them recognize and prioritize security alerts, vulnerability scans and incident reports.

Here are three key benefits of adding attack path management to your security tech stack.

1. Identify and critical assets and systems so you know where you need to focus and reduce risk.
2. Visually see all the attack paths associated with a particular alert and drill down for specific details.
3. Quickly get remediation recommendations and links to associated patches, data and tools.

Your security and network teams can now focus on the most important issues to reduce risk to your most important, business-sensitive assets.

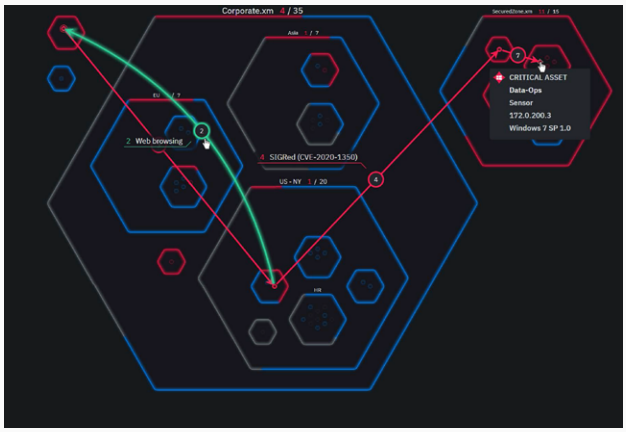
Protect your Cloud and Hybrid Environments

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.

Consider all the components required to build a successful cloud infrastructure: virtual machines, databases, connections to multiple services, as well as security roles and policies. There are many opportunities to make mistakes or misconfigure accounts and permissions. The result might expose your critical data to a wide audience outside your network. XM Cyber helps you understand your use of the cloud from attacker's perspective and put remediation in context based on risk.

Prioritize your Vulnerability Management

Using attack simulation in conjunction with vulnerability scanning, XM Cyber delivers continous visibility of all vulnerablities. 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.



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.

Select the Right Solution for Breach and Attack Simulation

XM Cyber's graph-based simulation technology continuously discovers the attack paths that lead to critical assets, enabling full visibility into organizational security posture. This allows users to understand how vulnerabilities, misconfigurations, user privileges etc. chain together to create a cyber-attack path to compromise critical assets.

The attack path management platform is capable of working across the hybrid cloud to identify exposures that could allow an attacker to pivot from an on-prem device to your cloud environment. It provides detailed prioritized, remediation guidance and can spot security issues that go unnoticed to direct and focus resources on what to fix first based on level of attack complexity and level of risk to critical assets.

About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Our attack path management platform continuously uncovers hidden attack paths to your critical assets across cloud and on-prem environments, so you can cut them off at key junctures and eradicate risk with a fraction of the effort. This approach is a complete game-changer, which is why some of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber 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
Paris: +33-1-70-61-32-76

xmcyber.com

XM Cyber