Integrating XM Cyber with Microsoft Defender for Endpoint (MDE) gives customers detailed information on potential attack paths that might result from a compromised system. By clearly identifying critical assets, the platform assists customers in fully understanding the potential impact of a breach and exactly what steps are required for remediation.

The combined capability improves visibility and lowers risk, helping customers prioritize security resources and focus on protecting their most critical assets.

The XM Cyber Attack-Centric Exposure Prioritization Platform (ACEPP) continuously identifies new exposures and attack vectors, prioritizes the cyber risks that affect business-sensitive systems and provides context-sensitive remediation options. And it allows the security and IT operation teams to achieve higher security posture and operational efficiency by focusing and remediating the cyber risks allowing attackers to breach business sensitive systems.

Working together, XM Cyber with Microsoft Defender for Endpoint (MDE) gives customers the ability to rapidly respond as a result of having a deeper understanding of the risks to critical business systems, laser-focused prioritization of exposures, and context-sensitive, least-effort remediation reporting.

Give Your Teams the Information They Need When They Need it

Security and IT teams can often be overwhelmed with alerts and vulnerability reports. The question is where do they start? What activities will have the greatest impact on improving security? Which assets are at risk because of an incident?

XM Cyber in combination with MDE helps solve these key challenges:

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

Prioritization of remedial actions is difficult due to the quantity of potential alerts. XM Cyber helps analysts understand the criticality of alerts based on tagging within the XM Cyber platform and the assets position relative to other attack paths.

Identifying the impact of lateral movement across the network is difficult. Acting as a virtual hacker, the XM Cyber platform shows all possible steps that can be taken from a particular asset identified through an alert in MDE.

No ability to identify choke points. XM Cyber clearly identifies assets that can affect multiple other assets, essentially creating a choke point. By eliminating the vulnerability of just one asset, the risk to the entire network can be greatly reduced.
Key Benefits of XM Cyber and MDE

Breach points and critical assets are easily identified

The XM Cyber Platform also helps users of Microsoft Defender for Endpoint to identify and tag their most critical assets. With this additional information, customers have a clear understanding of risk associated with alerts coming from Microsoft Defender for Endpoint. Combining efforts with threat and vulnerability management, the machine tagging is used to incorporate the risk appetite of an individual asset into the exposure score calculation. Therefore, machines marked as “high value” will receive more weight in the exposure score calculation.

Choke point identification

XM Cyber identifies assets on the network that can affect other assets. The more links to other assets, the greater the risk and the higher the priority must be to remediate.

Remediation Support

Rich, contextual information XM Cyber adds to the process of remediation prioritization indicates to customers whether or not they need to investigate deeper or give higher attention and priority when it comes to reducing risk. The combined capability improves visibility and lowers risk as more CISOs focus on applying security resources against their most critical assets.

Improved investigative process

Once suspicious activity is discovered with Microsoft Defender for Endpoint, the XM Cyber Platform explores and identifies the potential impact. By clearly identifying critical assets, the XM Cyber Platform assists customers in fully understanding how from a particular breach point the adversary might move laterally, reach other systems, or compromise critical assets.

Tagging is not generally used by customers of MDE. Since identifying and tagging assets is required in XM Cyber, analysts can use that information to identify the risk associated with any MDE alert.

Threat hunting using MDE is difficult without context. XM Cyber helps consolidate and put context into MDE to aid in investigations. By simulating an attack, the XM Cyber shows what would happen if an attacker had access to any particular asset. Analysts can be much more efficient in their threat hunting activities.

Weighted Scoring based on asset criticality

Combining efforts with threat and vulnerability management, the machine tagging is used to incorporate the risk appetite of an individual asset into the exposure score calculation. Therefore, machines marked as “high value” will receive more weight in the exposure score calculation.

Asset tagging and critical asset identification

Because the XM Cyber Platform helps users of Microsoft Defender for Endpoint identify and tag their most critical assets, security teams have a much clearer understanding of the risks associated with alerts coming from Microsoft Defender ATP. Asset tagging is mandatory in XM Cyber, it is not in MD.

Attack Simulation from any breach point

XM Cyber runs attack simulations automatically starting from the identified breach point showing you where an attack could go.

Validate the importance of MDE high, medium, and low alerts

Run attack scenarios using specific assets identified by MDE to evaluate the risk and potential impact a breach might have on the entire network.
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

Better Together – XM Cyber and MDE
XM Cyber provides better context for incident investigation and threat hunting via advanced attack simulation capabilities, allowing analysts to reduce investigation times and focus on improving security for systems and potential choke points that offer a clear attack path to critical assets. With both solutions working together, customers can not only review suspicious or high-risk device alerts, but also reduce risk from ancillary paths that could lead to business-critical assets, further enhancing the security team's ability to respond quickly.

XM Cyber is the global leader in Attack-Centric Exposure Prioritization that closes gaps in cloud and physical network security. Customers can rapidly identify and respond to cyber risks affecting their business-sensitive systems because the platform continuously calculates every potential attack path. Detailed remediation options are prioritized based on the potential impact, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber eliminates 99% of its customer's cyber risk by focusing IT and security operations on the one percent that represents the greatest threat.

“The rich, contextual information XM Cyber adds to the process of remediation prioritization indicates to customers whether or not they need to investigate deeper or give higher attention and priority when it comes to reducing risk.” says Tomer Teller, principal security program manager, Microsoft 365 Security. “The combined capability improves visibility and lowers risk as more CISOs focus on applying security resources against their most critical assets.”