XM Cyber for Cortex XSOAR

Enhance your security orchestration with the power of attack simulation

You've already made the smart decision to add orchestration to your security strategy. Now extend those capabilities with risk-free attack simulation and truly see every attack path available in your network.

Combining the power of XM Cyber with Cortex XSOAR gives you the extra context your teams require to make the best decisions concerning protecting your critical assets. Give them the tools they need to ask the important "what if" questions. XM Cyber shows exactly the attack paths leading to your most important data so you can stop attacks before they happen.

Security and network teams are constantly asking themselves whether a particular notice is high risk, low risk, affects mission critical assets, or something they can put off until the next patch comes out. By combining XM Cyber with the power of Palo Alto Networks Cortex XSOAR™, your teams can immediately understand the criticality of the assets involved and all attack paths associated with any incident.

Do You Have Attack-Centric Exposure Prioritization?

Simulating attacks generally means you are just testing security controls. That's not enough. Most analyst firms and security industry studies show that the greatest risk to enterprises today is not whether you've updated your patches or installed security in your network. The problems arise from human error and constantly changing network configurations. User mistakes, poor IT hygiene, misconfigurations, and misplaced credentials can be combined with other vulnerabilities to build an attack path that can go unnoticed by standard tools.

Attack simulations must include these exposures, or they'll leave your defenses open.

The next step in your Cortex XSOAR 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.

CORTEX XSOAR
BY PALO ALTO NETWORKS

Enrich Your Analysis With Contextual Information from XM Cyber

Your analysts rely on Cortex XSOAR for the best security incident orchestration possible. By adding the XM Cyber Attack-Centric Exposure Prioritization Platform (ACEPP), your teams gain additional information inside the incident page, including:

- Ability to answer a simple Yes or No whether business-sensitive critical assets are at risk
- The name and a description of the attack technique
- Detailed information on all affected assets, including which ones are deemed mission critical
- Identification of choke points – does this asset sit at the middle of many attack paths?
- Context-Sensitive remediation recommendations ranked in order of importance
- Hot link to the XM Cyber Platform for running attack simulations

Where necessary, XM Cyber will also create new incidents based on risk increasing at critical points in your network.

The bottom line is you need context. You need to continuously calculate every possible attack path, showing your security teams a visual representation that includes critical asset details and attacker techniques. By applying actual risk factors associated with your live environment, you improve your security and network operations ability to remediate the right incident in the right order.

Better Together – XM Cyber and Cortex XSOAR

By combining XM Cyber with Cortex XSOAR, you gain solid business results, lowering risk and stopping attacks. XM Cyber Labs estimates that customers can eliminate 99% of the real threats to your organization by solving the 1% that matters. Working together, you magnify the returns through increased contextual information that optimizes how your teams apply their time and resources.

XM Cyber enriches every incident with important risk-related data, such as whether the asset is noted as business-critical, is it a choke point in your network, and what other assets might also be at risk from lateral movement. A link is included that connects the incident to XM Cyber's platform, providing remediation details, and the visual attack simulation battleground showing all available attack paths.

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