XM Cyber Solves Multiple Security Problems Check Out These Use Cases

Most organizations work diligently to constantly manage and evaluate their cyber security risk. Typically, vulnerability management processes are implemented, security controls installed, and penetration testing or red team exercises are performed to assess and reduce risk.

However, the challenges with these practices remain and generally consist of prioritizing remedial projects, understanding the context of internal network vulnerabilities, misconfigurations of controls, and point-in-time testing that does not keep up with everyday changes to a network.

This is what attackers are exploiting.

XM Cyber helps organizations continuously see their environment from an attacker's perspective. The platform exposes how vulnerabilities, misconfigurations and user behaviors can be combined to form a chain of attack that can reach critical assets.

More importantly, it provides the prioritized remediations necessary to close those gaps to defenders.

Here are some examples of how customers are using the platform.

Critical Asset Risk Visibility

In every organization there are crown jewels that are critical to the operation and continuity of the business. Understanding the risk to those assets is critical in prioritizing security team efforts.

Automated Red Team

Enable any team with the ability to see how an attacker would traverse to a crown jewel regardless of red team expertise. Simply pick an asset and the attacks are calculated automatically.

Continuous Validation

Networks are dynamic and so should be the testing. XM Cyber enables continuous validation of risk to your assets as your network evolves.

Prioritized Remediation

Go beyond just finding vulnerabilities. Get a comprehensive plan to remediate security gaps based on context and a holistic view of your network. XM Cyber incorporates IT hygiene, vulnerabilities and user behaviors that combined can lead to a compromise. Save time and effort for your team by pinpointing exactly which remediations have the greatest impact.

Network Segmentation

If you are investing in network segmentation or zero-trust network architecture, you need a way to identify if a segment has gaps or if a change has put assets at risk. Is your segmentation the same it was when you implemented it? How do vulnerabilities and user behaviors add risk?

OT Environments: Identify user behaviors, network misconfigurations and other attack vectors that allow access to OT environments.

PCI Networks: Identify how PCI networks can be accessed and data compromised continuously.

Healthcare: Identify how an attacker can compromise and affect the devices on the network and reduce exposure to critical systems.

Real Time Attacker Visibility: React to any changes that expose risk to your network and assets.

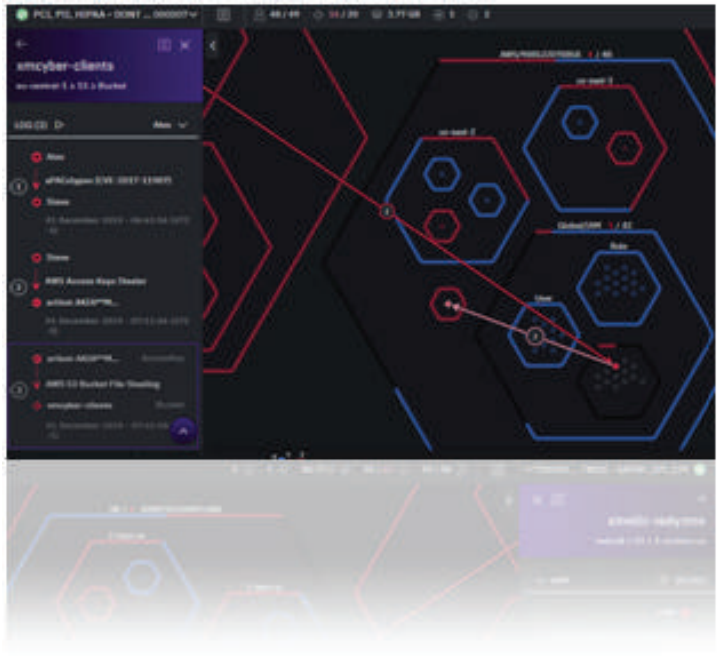
AWS Cloud Exposure

AWS and cloud adoption have left many organizations wondering about their security. XM Cyber helps by showing how secure your data in the cloud is, and how to assess the risk of assets in the cloud.

Privilege Escalations: Cloud policies for users, roles and groups can allow for escalations due to misconfigurations. XM Cyber can identify issues in one account or cross-account attacks.

Validate Resource Access: Identify how an attacker can access an S3, Lambda, or other resources through continuously testing.

Hybrid Attacks: Identify how attackers can compromise on-premise devices and then move to assets in the cloud.



"XM Cyber helps organizations continuously see their environment from an attacker's perspective. The platform exposes how vulnerabilities, misconfigurations and user behaviors can be combined to form a chain of attack that can reach critical assets."

Active Directory Infrastructure

Active directory is the heart of many organizations and attackers that can compromise key Active Directory infrastructure and cause widespread damage.

Domain Controllers: Identify how domain controllers can be compromised and how to protect against group policy attacks, credential harvesting methods, golden ticket, and others.

DNS/DHCP/Proxy Servers : Identify easy and sophisticated attacks that can hijack DNS, DHCP and Proxy resolution.

Active Directory Hardening: Reduce overall network risk by hardening your AD environment with pinpointed remediations from excessive permissions to misconfigured services and more.

APT and Threat Prevention

Constant attacks against organizations requires constant assessment and response. Closing the gaps from missed vulnerabilities, IT hygiene issues, misconfigurations and us behaviors reduce the possibilities for the attacker.

MITRE ATT&CK: XM Cyber maps TTPs that are possible ir your environment to easily digest by security teams.

APT Simulation : Identify which attacks APTs can use that go under the radar not triggering alerts and bypassing security controls.

Attack Surface: Reduce the attack surface in your enviror ment by identifying the underlying and root cause of the attacks that are possible prior to an attacker exploiting the

Compliance Maintenance

Identify the risks associated with your devices and networks requiring compliance and enable automated risk reduction to successfully pass penetration tests associated with those compliance tests.

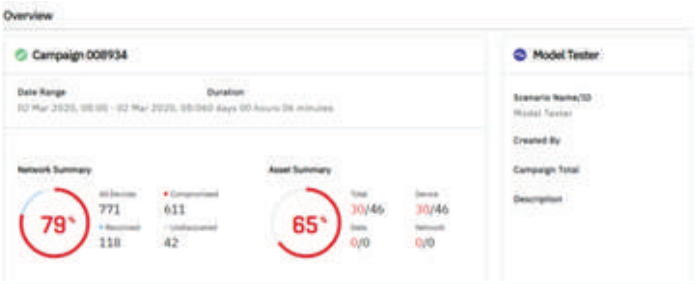
Maintain Compliance: Continuously assess if risks expose your devices to compliance violations.

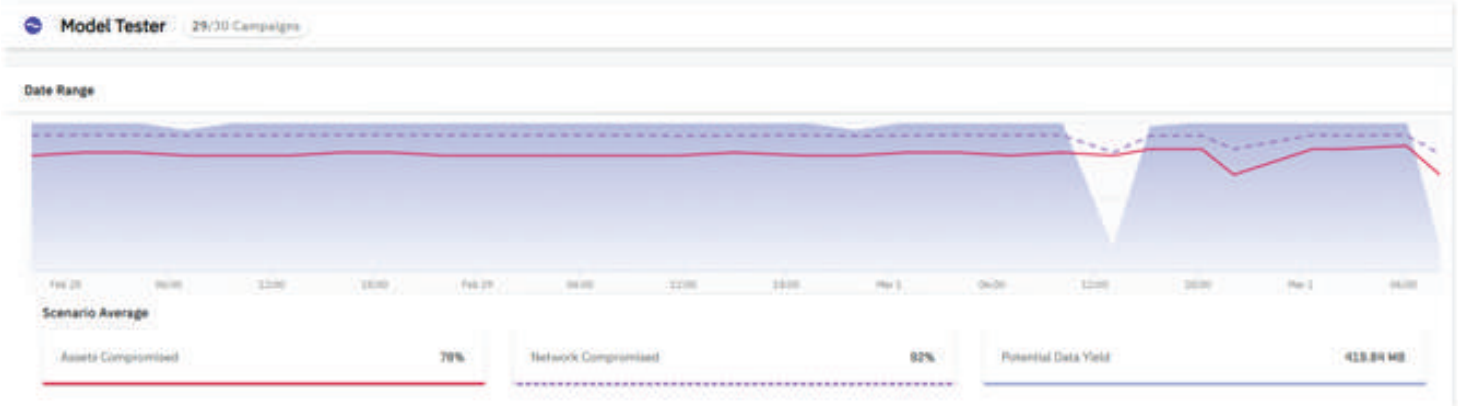
Continuous Testing: Monitor your compliance after a pen test to validate that implementations of remediations are effective and that new ones do not put your compliance at risk.

Risk Reporting

Reporting on the risk of your critical assets to senior leadership is important to help guide the direction of investments in technology and personnel.

XM Cyber generates reports that provide an in-depth risk model by incorporating vulnerabilities, IT hygiene, misconfigurations and user behaviors so you can understand the risk from an attacker's perspective.





Risk Identification: Generate reports based on business use cases. Identify how data, systems, and networks can be compromised and export remediation reports

Continuous Validation : View trendlines and risk quantification to understand if the changes in your environment are making a difference in reducing risk or if new attack vectors increase risk.

Conclusion: To find out more and get a free assessment, please reach out to info@xmcyber.com or visit https://xmcyber.com/book-a-demo

About XM® Cyber

XM Cyber provides the first fully automated breach and attack simulation (BAS) platform to continuously expose attack vectors, from breach point to any organizational critical asset. This continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of security gaps. In effect, XM Cyber operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of the attack. XM Cyber has already received over 20 industry awards, including being recognized as a "Technology Pioneer" by the World Economic Forum. XM Cyber's customers include leading financial institutions, critical infrastructure organizations and manufacturers across North America, Europe, and Israel.

XM Cyber was founded by the highest caliber of security executives from the elite Israeli intelligence sector. Together they bring a proven track record in both the offensive and defensive cybersecurity domain. The company is headquartered in Israel and has offices in the US, UK and Australia.

XM CYBER

Tel Aviv +972 3 978 6668 New York +1 866 598 6170 Sydney +61 2 8880 0705 London +44 203 322 3031 info@xmcyber.com