XM Cyber | SOLUTION BRIEF

XM Cyber Identity Exposure Management

Continuously Monitor For Identity And Access-Related Exposures Across Your Hybrid Environments. Remediate Validated Attack Paths Before Attackers Can Exploit Them.

Identities are prime targets for bad actors looking to compromise an organization's business critical assets. They exploit issues such as Active Directory users with excessive privileges, MFA not being enabled or stolen credentials that they have acquired.

Which means security teams need to be constantly monitoring for these types of issues across the sprawling, frequently changing identity attack surface.

XM Cyber continuously monitors for identity exposures across on-premises, cloud and hybrid environments such as issues and misconfigurations that attackers can leverage to compromise business-critical assets. Potential attack paths are validated against thousands of attack techniques to prove they can be exploited in the real world and prioritized so busy teams know what to fix first.

Uncover Identity Exposures

Get continuous visibility of identity risks and misconfigurations across hybrid environments.

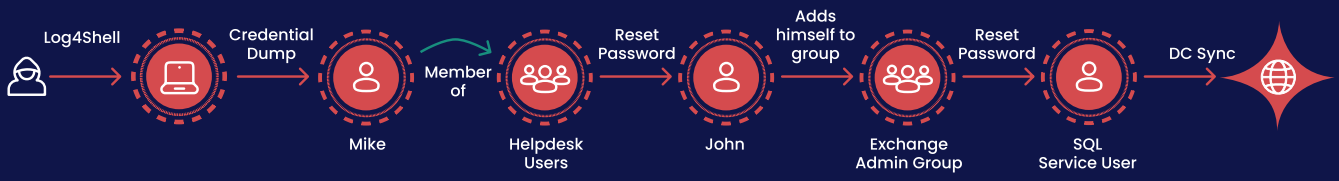
Act for Maximum Impact

Prioritize remediation of identity-related exposures that are exploitable and lead to business-critical assets.

Communicate Risk Effectively

Give remediation teams the context, guidance and evidence they need to drive action.

How Identity Exposures can Lead to Critical Asset Compromise



How XM Cyber Protects Against Identity Exposures

XM Cyber leverages Attack Graph Analysis™ to provide end-to-end visibility into the threats (including from identities) targeting an organization's most critical assets. Here's how it works:

Comprehensive Attack Mapping

Continuously map attack paths, showing how exposures can lead to high-value business assets.

Prioritized Risk Management

Start by fixing high-impact exposures that are validated and can cause asset compromise.

Identity Security Posture

Analyze a wide range of issues including excessive privileges, Active Directory tiering and misconfigurations such as MFA not being enabled.

Exposed Credential Management

Get near real-time alerts about stolen credentials and understand how they compromise your critical business assets.

Security Controls Monitoring

Monitor security tools for misconfigurations and compliance violations.

Guided Remediation

See detailed steps on how to remediate an issue with alternative options where required.

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.