XM Cyber | SOLUTION BRIEF

Prevent Identity - Based Attacks

Stop bad actors from using excessive permissions, credentials and misconfigurations to compromise your business-critical assets.

Identities are prime targets for bad actors looking to compromise an organization's business critical assets. They exploit issues such as human, AI and machine 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 for 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

Continuously map identity risk and lateral movement across the full attack surface, from on-premises to cloud.

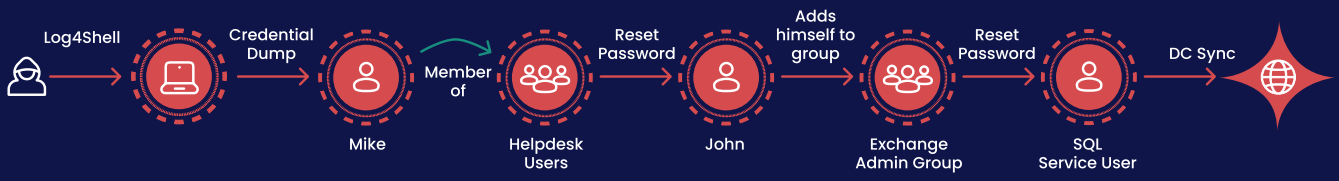
Eliminate the Identity Risks That Matter

Prioritize validated attack paths that exploit identity exposures to compromise critical assets and sensitive data.

Articulate Risk, Drive Remediation

Communicate identity risk effectively to drive urgency across teams and prove security posture and ROI to management.

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 and exploitability - based exposure prioritization across complex, hybrid environments. Here's how it works:

Eliminate Identity Exposures

Remediate exposures across hybrid environments, understanding how identity risks interconnect to form attack paths to critical assets.

Assess Security Posture

Gain deep insight into Active Directory and cloud identity and access exposures, resource configuration and security posture.

Enforce Least Privilege Access

Maintain a holistic view of Active Directory and cloud permissions (CIEM) and their usage to speed preventative security hygiene.

Understand Risk From Credentials

See where domain and local credentials are cached or reused and if credentials have been exposed.

Monitor Identity Security Tools

Detect configuration drift over time, ensure optimal performance and align with regulatory frameworks.

Mobilize and Fix Faster

Prove urgency with business impact prioritization of issues, and speed the fix with guided remediation steps.

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.