Use Case

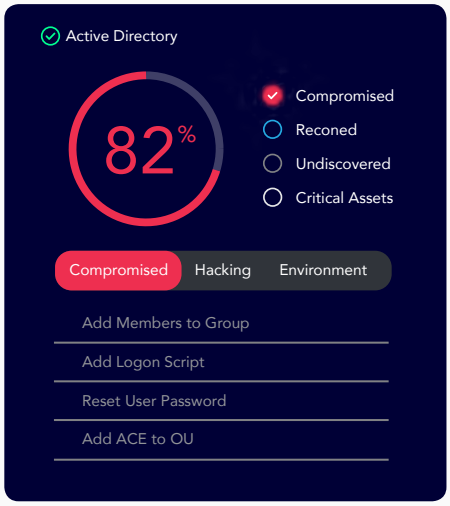
XM Cyber | See All Ways™

XM Cyber for Active Directory

Discover Active Directory exposures within a single consolidated attack path to increase your cyber resiliency

Microsoft's Active Directory (AD) is widely used by enterprises around the world to connect and manage individual endpoints inside corporate networks. Making matters worse, AD is a top target for attackers seeking to obtain domain admin-level access. The use of AD is so common that approximately 90% of the Global Fortune 1000 companies use it as a primary method to provide seamless authentication and authorization. An attacker that has compromised an AD user could use this to:

- Elevate privileges
- Conceal malicious activity in the network
- Achieve persistency by using AD capabilities to execute malicious code
- Make their way into the cloud environment to compromise assets, particularly Azure because of the inherent trust relationship between the two.



With a much faster time-to-compromise and a low complexity to execute, this significantly increases the scope and damage of the attack and compromise to an organization's critical assets.

Active Directory abuse goes unseen in organizations' due to the inherent nature of dynamic configuration issues in addition to keeping it updated - this blind spot - of what seemingly looks secure but poorly configured puts organizations at risk as traditional siloed security tools cannot identify the risk and potential compromise of critical assets in the network.

According to Gartner, it is critical to make concentrated efforts to comprehensively secure and monitor AD, proactively look for threats and misconfigurations, and remediate to prevent dangerous actions from taking place

Continuously Disrupt AD Risks Across On-prem and Cloud Environments

XM Cyber's Attack Path Management platform is the first in the industry to provide holistic Active Directory security to find and fix weaknesses before the attack takes place. Organizations can now see how secure their Azure environments are from Active Directory originated breaches. XM Cyber shows how Active Directory abuse comes into play in the entire attack path, bringing multiple attack techniques together to pinpoint highest risks and offer step-by-step remediation guidance.

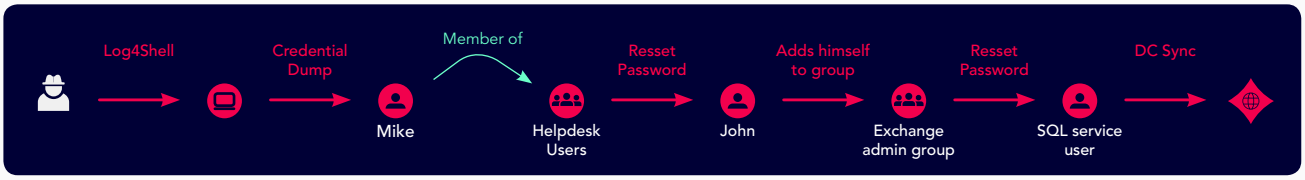
Key Benefits of the XM Cyber Attack Path Management Platform:

Continuously eradicate Active Directory risks across on-prem and cloud environments - Discover how attackers can move laterally in the network through impersonating an AD user, escalating privileges allowing them to run malicious code in the network covertly, and even gain access to the cloud environment by moving from a compromised enterprise AD user to his joined Azure AD user.

Extensive Attack Technique Arsenal for Active Directory and Azure AD - Including privilege escalation in Active Directory, credential grabbing/dumping, vulnerabilities and taking advantage of misconfigurations and legitimate structuring of your Active Directory users, services, computers, and even files.

Prioritized Remediation for all Active Directory changes and malicious threats - Highlight the riskiest credentials and permissions across users, endpoints and services managed in your Active Directory, enabling you to direct resources to remediate the most impacting risks first with step-by-step guidance. Enrich your SOC, SIEM or SOAR with attack path insights to quickly prevent attacks.files.

Comprehensive Security Posture Analysis reflecting Active Directory weaknesses in real time
- Continuous security score that directly correlates with the likelihood of an attack that can compromise your critical assets based on the entirety of your environment and what's managed by Active Directory



Active Directory Security Features with the Attack Path Management Platform

Security Score with visibility to see how secure your environment is from Active Directory originated breaches in a single consolidated attack path

Attack paths include all hidden connections between misconfigurations, vulnerabilities and over permissive users in enterprise and cloud

Focus on business-critical assets like endpoints, financial DBs, and multiple cloud entity types (S3, Lambda, roles) vs technological assets like domain admins and domain credentials to reveal impact on the organization

Prioritized remediation based on choke points (disrupting many attack paths through least number of actions for highest impact)

End-to-end attack path visualization for easy understanding and quick remediation across the hybrid environment

Comprehensive repository of AD attack techniques for accurate attack path modeling

XM Cyber's solution demonstrates how AD abuse comes into play across the entire attack path, bringing multiple attack techniques together to pinpoint the riskiest credentials and permissions across users, endpoints and services managed in AD, while offering prioritized, step-by-step remediation guidance.

About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Its attack path management platform continuously uncovers hidden attack paths to businesses' critical assets across cloud and on-prem environments, enabling security teams to cut them off at key junctures and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber 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
Paris: +33-1-70-61-32-76

xmcyber.com

XM Cyber