XM Cyber

# Active Directory
## Security Checklist

Active Directory is Microsoft's database and services that is responsible for connecting users with network resources. Active Directory is crucial in Windows-based environments, enabling organizations to centrally manage and organize users, computers, and other types of devices. It contains critical information regarding the environment, such as the users and computers, and the permissions each user has been granted.

Given its central role in authentication and authorization, it's also a prime target for attackers.

This is why it's absolutely essential to secure user credentials, systems, sensitive data, software, and applications and protect them from unauthorized aaccess. If an organization's Active Directory is breached, it will inevitably weaken the integrity of the overall security posture.

## Active Directory Security Best Practices

- [ ] **Limit the use of Domain Admins and other Privileged Groups:** Minimize the number of accounts with privileged access to reduce the attack surface.
- [ ] **Use at least two accounts per User:** Implement a separate standard user account for regular activities and a privileged account for administrative tasks.
- [ ] **Secure the domain administrator account:** Apply strong password policies, enable account lockouts, and regularly monitor for any unauthorized access attempts.
- [ ] **Disable the local administrator account (on all computers):** Remove unnecessary administrative privileges to limit potential vulnerabilities.
- [ ] **If you do use it, enable Laps:** Implement the Local Administrator Password Solution (LAPS) to securely manage local administrator passwords.
- [ ] **Use a secure admin workstation (SAW):** Establish a dedicated workstation with strict security controls for administrative activities.
- [ ] **Enable audit policy settings with group policy:** Set up comprehensive audit policies to track and record security events for later analysis.

- [ ] **Monitor for signs of compromise:** Employ intrusion detection systems, security information, and event management solutions to proactively identify and respond to any security incidents.
- [ ] **Ensure proper password complexity:** Encourage the use of longer passphrases instead of complex passwords to enhance security.
- [ ] **Use descriptive security group names:** Organize security groups with meaningful names to simplify access management and administration.
- [ ] **Lock down service accounts:** Apply least privilege principles to service accounts and limit their privileges to only what is required for specific tasks.
- [ ] **Do not install additional software or server roles on DCs:** Use domain controllers exclusively for their intended purpose and avoid unnecessary installations to reduce attack vectors.
- [ ] **Find and remove unused user and computer accounts:** Regularly audit Active Directory to identify and disable or delete accounts that are no longer in use.
- [ ] **Remove Users from the Local Administrator Group:** Remove non-administrative users from the local administrator group to minimize potential security risks.
- [ ] **Employ patch management and vulnerability scanning:** Regularly apply security patches to all systems and perform vulnerability scans to identify and remediate any weaknesses.
- [ ] **Use secure DNS services to block malicious domains:** Utilize DNS-based threat intelligence and filtering services to prevent access to malicious domains.
- [ ] **Run supported operating systems/protocols:** Keep systems up to date with supported and patched versions of operating systems and protocols to avoid known vulnerabilities.
- [ ] **Use two-factor authentication by protocol:** Implement additional authentication measures, such as two-factor authentication, for critical protocols to enhance security.
- [ ] **Monitor DHCP logs for connected devices:** Analyze logs from DHCP servers to detect any device connections, unauthorized access, and irregular network behavior.
- [ ] **Leverage AD attack path analysis:** Gain a full understanding of the chain of privileges and actions that can be abused, which can allow attackers to compromise accounts.
- [ ] **Monitor DNS logs for malicious network activity:** Monitor DNS logs to help optimize network performance, and identify and address potential threats.
- [ ] **Create a recovery plan:** This will help prevent data loss and ensure business continuity.

# How Can XM Cyber Help Keep Your Active Directory Secure?

XM Cyber demonstrates how Active Directory abuse comes into play throughout the entire attack path, bringing multiple attack techniques together, to pinpoint the most impactful risks and offer step-by-step remediation guidance.

### Proactive Active Directory Risk Analysis In Real Time

Continuously analyze your security score to understand 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.

### Improve Security Response for All Active Directory

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 impactful risks first, with step-by-step guidance. Enrich your SOC, SIEM or SOAR with attack path insights to quickly prevent attacks.

### Prevent Active Directory-Related Attacks Across On-prem and Cloud Environments

Discover how attackers move laterally by impersonating Active Directory users, escalating privileges and allowing them to run malicious code in the network covertly, and even gaining access to cloud environments by moving from compromised enterprise Active Directory users to the associated Azure Active Directory user.

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia, and Israel.