XM Cyber

Identity and Access Security Checklist

Identities and access permissions are the highways that connect every corner of an organization's environment - making them a critical component of cybersecurity, and prime targets for threat actors.

This checklist provides an overview of some of the key areas to consider when assessing your current identity and access security posture.

Best Practices

- [ ] **Maintain onboarding hygiene:** Check that new identities are not cloned from templates with privilege creep and take time to understand what access needs really are
- [ ] **Ensure password complexity:** Enforce best practice password requirements for all users
- [ ] **Use strong encryption for passwords:** Do not allow cleartext passwords or outdated encryption techniques
- [ ] **Eliminate shadow identities:** Identify and remove accounts that are no longer required (e.g. the user has left) and may have been forgotten
- [ ] **Implement account tiering:** A vital practice for Active Directory that reduces the risk of lateral movement and credential theft
- [ ] **Check group memberships:** Only add users that need to be in a group, especially groups with elevated permissions (e.g. admin groups)
- [ ] **Reset compromised credentials:** Identify credentials that have been exposed by a threat actor (e.g. in a data breach or infostealer in your environment)
- [ ] **Remove cached credentials:** See where credentials have been cached on a device and could be exploited
- [ ] **Identify shared credentials:** Understand where users have reused credentials across different accounts and remediate them
- [ ] **Check IAM/PAM/IGA configuration:** Make sure that identity security tools are configured to best practices and catch unintended changes over time
- [ ] **Enforce least privilege access (LPA):** Check that elevated permissions are actually being used (e.g. CIEM/Active Directory permissions) and remove if not needed
- [ ] **Privileged access hygiene:** Make sure admins log on from a secure device and only use admin accounts for tasks that require them
- [ ] **Map the full environment:** In hybrid and multi-cloud environments assess where permissions might allow unintended cross-platform access (e.g. from AD/Entra to Azure or AWS)

- [ ] **Perform compliance checks:** Connect identity controls to specific frameworks and regulations to maintain compliance and audit readiness
- [ ] **Map and monitor non-human identities (NHI):** Machine and AI identities often have elevated permissions with less oversight over their activities
- [ ] **Detect configuration drift:** See when a security setting like “Allow Public S3 Buckets" is unintentionally enabled even when it was correctly configured (turned off) at first
- [ ] **Understand the real business impact:** See how threat actors combine identity exposures, CVEs, misconfigurations and more to reach critical assets
- [ ] **Run continuous monitoring:** Catch issues before attackers can exploit them by continuously monitoring your identity and access landscape
- [ ] **Share intelligence and strengthen posture:** Integrate exposure data with your SOC, SIEM or SOAR tools to boost overall security posture
- [ ] **Keep regular backups:** Continuously verify that Active Directory or cloud identity backups are encrypted, offline, and restorable

How XM Cyber Helps Boost Your Identity and Access Security

XM Cyber shows how identity and access exposures can be exploited by threat actors in combination with other issues such as CVEs and misconfigurations to compromise your business critical assets. It enables you to prioritize effectively and take action fast with guided remediation.

Uncover Identity Exposures

Continuously map identity risk and lateral movement across the full attack surface, from on-premises to cloud. Credentials, configuration drift, inappropriate access permissions and more are examined holistically across your organization’s attack surface.

Eliminate the Identity Risks That Matter

Prioritize validated attack paths that exploit identity exposures to compromise critical assets and sensitive data. Every path is tested for exploitability so you know which areas to focus on, minimizing time spent on investigation and maximizing security return on investment.

Articulate Risk, Drive Remediation

Communicate identity risk effectively to drive urgency across teams and prove security posture and ROI to management. Effective prioritization, justification and guided remediation simplifies the mobilization process and speeds risk reduction.