CROWDSTRIKE

ACTIVE DIRECTORY SECURITY ASSESSMENT

Comprehensive review of your Active Directory components and prioritized actionable recommendations

CROWDSTRIKE SERVICES: ACTIVE DIRECTORY SECURITY ASSESSMENT — SECURE YOUR AD

One of the serious threats organizations face is attackers using Active Directory configurations to identify attack paths and capture privileged credentials so they can deeply embed themselves into target networks.

CrowdStrike® Services offers an in-depth review of your Active Directory configuration and Group Policy Object (GPO) settings in order to assess security configuration issues attackers can leverage during a breach. The assessment involves review of documentation, discussions with your staff, execution of proprietary tools and manual review of your Active Directory configuration and settings. CrowdStrike also leverages the Falcon platform to understand how attackers are operating in Active Directory environments.

THE ASSESSMENT PROCESS HAS THREE PRIMARY PHASES:

1. **Gather data from the environment, while on-site or remote**
2. **Interpret and analyze the results**
3. **Complete the assessment report and provide detailed recommendations**

KEY BENEFITS

- Provides a snapshot of the Active Directory security configuration as of a point in time
- Identifies the most common and effective attack vectors and explains how best to detect, mitigate and prevent them
- Offers tailored recommendations for leveraging existing technology investments to improve your organization's overall security posture
- Customizes Active Directory security best practices to align with business processes and requirements and to minimize impact
- Identifies top security issues and provides guidance on the best methods to mitigate and resolve them
- Provides a detailed report of the issues discovered and their impact along with recommended remediation
- Delivers a plan of action that includes resolution and mitigation recommendations for the identified issues

KEY ASSESSMENT AREAS

CrowdStrike's Active Directory security assessment can be performed at any time. It can be conducted proactively to help your organization fix issues before penetration testing; after penetration testing to better help you understand what happened; or as part of a yearly maintenance project to fix issues identified during infrastructure updates.

1. CONFIGURATION VISIBILITY AND MANAGEMENT

- Perform Active Directory forest and domain trust configuration and security review
- Conduct domain controller management review including operating system versions, patching, backup and server lifecycle management
- Identify domain controller auditing configuration and review event central logging system

2. GROUP POLICY AND PRIVILEGE CONTROLS

- Review Active Directory administration groups (users, service accounts, etc.)
- Discover custom security groups with privileged access to Active Directory
- Enumerate Active Directory organizational unit (OU) permissions with a focus on top-level domain OUs

3. RECOMMENDATIONS AND ACTION PLANS

- Highlight Active Directory security misconfigurations and recommend specific remediation/mitigations
- Provide recommendations for domain controller auditing and determine the specific event IDs that should be sent to the central logging system or SIEM
- Provide broad recommendations for all Windows system auditing (specific event IDs) that should be forwarded to the central logging system or SIEM

A SECURE ACTIVE DIRECTORY ENVIRONMENT CAN MITIGATE MOST ATTACKS.

Most attacks today can be mitigated by securing key Active Directory components. Local administrator accounts, host-based firewalls and user group identification are a few of the components enumerated. CrowdStrike's Active Directory Security Assessment covers all of these components and more, and provides recommendations to help organizations secure their infrastructures.

CROWDSTRIKE

CrowdStrike® is the leader in cloud-delivered endpoint protection.
The **CrowdStrike Falcon®** platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at **crowdstrike.com**