

ACTIVE DIRECTORY SECURITY ASSESSMENT

Comprehensive review of your Active Directory security components

ACTIVE DIRECTORY CONFIGURATIONS ARE A SERIOUS THREAT

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

EVALUATE THE SECURITY OF YOUR ACTIVE DIRECTORY

CrowdStrike® Active Directory Security Assessment is a unique offering designed to review your Active Directory configuration and policy settings to reveal the security configuration issues attackers can leverage. The assessment involves review of documentation, discussions with your staff, execution of proprietary tools and a manual review of your Active Directory configuration and settings. You receive a detailed report of the issues discovered and their impact along with recommended steps for mitigation and remediation.

THE ASSESSMENT PROCESS HAS THREE PRIMARY PHASES:

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

KEY BENEFITS

Provides a snapshot of the Active Directory security configuration at 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 minimize impact

Identifies top security issues and provides guidance on the best methods to mitigate and resolve them

Delivers a plan of action that includes resolution and mitigation recommendations for the identified issues

KEY SERVICE FEATURES

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.

CONFIGURATION VISIBILITY AND MANAGEMENT

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

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

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 security information event management (SIEM)
- Provide broad recommendations for all Windows system auditing (specific event IDs) that should be forwarded to the central logging system or SIEM

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at www.crowdstrike.com/services/

Email: services@crowdstrike.com

© 2022 CrowdStrike, Inc. All rights reserved.

WHY CHOOSE CROWDSTRIKE?

Expertise: CrowdStrike's Active Directory Security Assessment tools and process were developed by a Microsoft Certified Master in Active Directory.

Comprehensiveness: The extensive, action-focused security review delivers insight and summarizes the critical items that need work. The assessment is focused on mitigation and practical recommendations for how to stop attackers leveraging Active Directory.

Relevance: The tools and methodology are constantly assessed and refreshed to take into account new attack approaches and reflect best practice and published research.

