CrowdStrike Services

TRIMARC

CROWDSTRIKE

Data Sheet

ACTIVE DIRECTORY SECURITY ASSESSMENT

Enhance the cybersecurity posture of your Microsoft Active Directory

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

The Active Directory Security Assessment is designed to review your Active Directory configuration and policy settings to reveal any security configuration issues that attackers could leverage to gain access to your network. 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 provides a snapshot of the Active Directory security configuration and identifies the most common and effective attack vectors and explains how best to detect, mitigate and prevent them. The output of the assessment offers tailored recommendations for leveraging existing technology investments to improve your organization's overall security posture. We customize our Active Directory security best practices to align with your business processes and requirements. We identify the top security issues and provide guidance on the best methods to mitigate and resolve them.

KEY BENEFITS

Establish a plan of action that includes resolution and mitigation recommendations for identified issues in your Active Directory

Better protect your organization from identity-based threats and the misuse of user credentials

KEY SERVICE FEATURES

The Active Directory Security Assessment is a partner-delivered service from Trimarc. The assessment is conducted proactively to help your organization fix issues before running a penetration test; 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.

The assessment includes:

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 domain controller auditing configuration and review 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 recommendations for all Windows system auditing (specific event IDs) that should be forwarded to the central logging system or SIEM

ABOUT TRIMARC

Trimarc is a professional services company that helps organizations secure their Microsoft platform, both on-premises and in the cloud. Trimarc is on a mission to help organizations better secure their critical IT infrastructure by focusing on a "reality-based security model" which targets attacker tactics and how to best stop them. Trimarc identifies security issues in an organization that attackers could exploit to fully compromise the environment and provides custom recommendations to effectively mitigate these issues.

CONTACT CROWDSTRIKE

CrowdStrike: **We stop breaches.**

Learn more: **www.crowdstrike.com/services/**

Email: **services@crowdstrike.com**

Request information: **click here**

WHY CROWDSTRIKE PARTNERS WITH TRIMARC

CrowdStrike has established an ecosystem of trusted partners to deliver expertise and capacity in key areas of cybersecurity.

Deep Microsoft Expertise: Trimarc tools and processes were developed by a Microsoft Certified Master in Active Directory.

Comprehensive Security Analysis: Trimarc performs a comprehensive analysis of your Active Directory security posture.

High-Priority Findings: Trimarc discovers high-priority findings and provides feasible, actionable recommendations to get issues fixed.