FIREEYE™

数据表

# Active Directory Security Assessment (活动目录安全评估)

## 移除 Active Directory (活动目录) 错误配置、流程弱项及开发方法的风险

### 优势

- 了解组织 Active Directory 环境的当前状态
- 主动解决常见的 Active Directory 配置不当和设置不当的问题
- 强化常见攻击面，降低安全事件的风险和影响
- 实施更严格的策略，最大程度减少特权访问
- 增强 Active Directory 内的观察和检测能力
- 战略性改进 Active Directory 基础结构的整体安全状态

**为何选择 FireEye Mandiant**

自 2004 年起，FireEye Mandiant 始终走在网络安全防护和网络威胁情报领域的前列。我们的事件响应产品不断用于处置全球最复杂的违规事件。我们通过结合对手、设备及受害者情报资源，深入了解威胁制造者及其快速多变的策略、技术及程序 (TTP)。

我们的活动目录安全评估 (ADSA) 的开发基于丰富的事件响应经验、全球抑制及修正服务，以及对新兴威胁情报的了解。

我们通过成熟的测试和审查技术进行评估，进而得到实用性的指南和建议，成功消除客户环境中的攻击者，且有助于修正受到威胁的部分。

各组织可通过该主动性方法，改进 Active Directory 的安全状态，避免出现因 Active Directory 环境常见弱点而导致的事件。

**概要**

随着技术的进步和组织的发展，Active Directory 的维护愈加复杂和繁琐。组织通常难以适当维护原有配置，亦无法保证 Active Directory 始终配备最新的安全增强功能。

ADSA 评估过程中，Mandiant 可帮助您的组织改进必要的关键流程、配置标准、安全及监测控制，以有效保护 Active Directory 环境以及其支持的基础结构。

**我们的方案**

Mandiant 专家与客户组织的主要利益相关者合作，执行一系列站内操作，根据当前技术和流程执行数据收集和脚本输出分析。我们的专家将这些信息用于评估体系结构 (包括本地环境和云环境)，并确定 Active Directory 基础结构中可能存在的攻击路径。

Mandiant 顾问提出特权用户访问和特权访问管理的强化方式，增强 Active Directory 内恶意活动的观察和检测能力，提供建议的战略路线图，以改善客户 Active Directory 基础结构的整体安全状态。

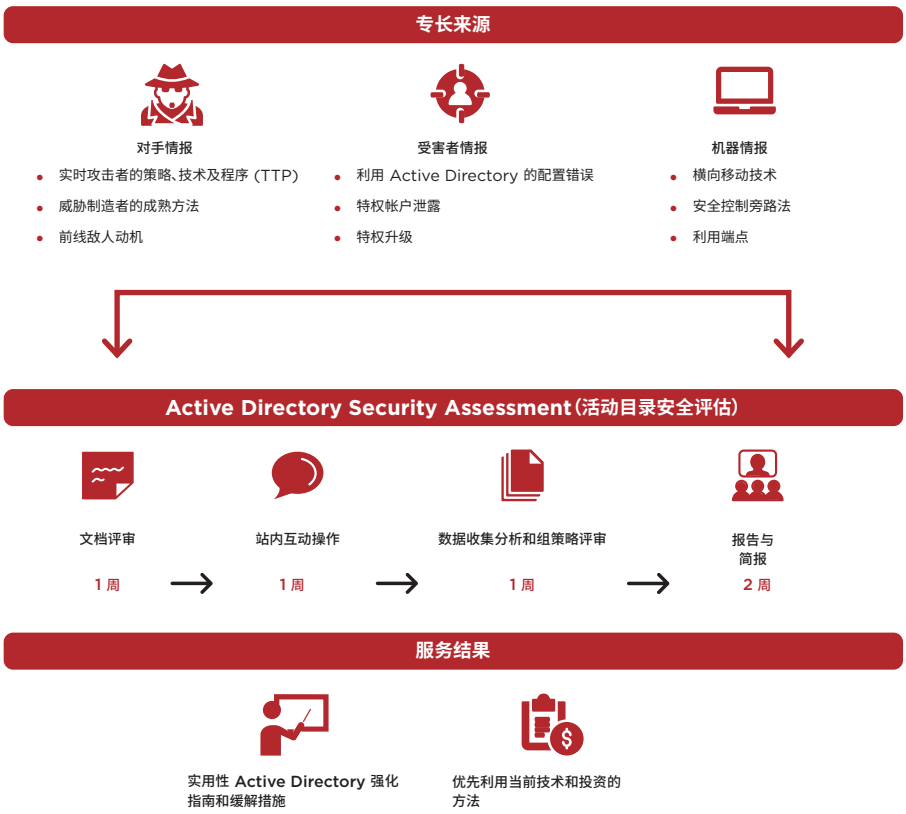


**图 1.** 服务周期

## ADSA 重点领域

- Forest（森林）基础结构与信任关系
- 操作流程
- 监测和响应
- 特权帐户与访问管理
- Group policy（组策略）控制和实施
- 权限委派
- 服务帐户与服务主体名称 (SPN)
- 远程访问控制与强化
- 端点配置与强化
- 与 Microsoft Azure 和 Microsoft Office 365 集成

## 交付项目

评估结束后的详细报告包含：

- 当前环境的 Active Directory 安全配置快照
- 与当前技术和操作流程保持一致的特定 Active Directory 安全最佳标准
- 有关限制、管理和监测环境中的特权用户访问和帐户的实用性建议
- 有关进一步强化 Active Directory 基础结构安全状态的详细建议

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com/services**

**FireEye**
26/F Times Square, 93 Middle Huaihai,
Huangpu Shanghai, China
china@fireeye.com



**关于 FireEye, Inc.**
FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的讯息安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。