

Active Directory Security Assessment

Benefits:

- Gain visibility into the current state of an organization's Active Directory environment
- Proactively mitigate commonly exploited Active Directory misconfigurations and settings
- Reduce the risk and impact of a security incident by hardening a common attack surface
- Implement stricter policies to minimize privileged access
- Increase visibility and detection within an Active Directory environment
- Strategically improve the overall security posture of the Active Directory infrastructure

Mitigate the risk of Active Directory misconfigurations, process weaknesses and exploitation methods

Why Mandiant

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of threat actors and their rapidly changing tactics, techniques and procedures (TTPs) by leveraging our combined adversary, machine and victim intelligence sources.

Our Active Directory Security Assessment (ADSA) was developed based on extensive incident response experience, global containment and remediation services, and emerging threat intelligence.

The practical guidance and recommendations derived from this assessment reflect tested and vetted techniques that have successfully eradicated attackers from client environments and helped remediate threats.

By using this proactive methodology, organizations can enhance their Active Directory security posture and protect against incidents that exploit common weaknesses in an Active Directory environment.

Overview

Active Directory can be complex and cumbersome to maintain, especially as technologies and organizations evolve. Organizations often struggle to properly maintain configurations and keep current with the latest security enhancements of Active Directory.

During an ADSA, Mandiant helps your organization improve the key processes, configuration standards, security and monitoring controls required to effectively secure an Active Directory environment and its supporting infrastructure.

Our approach

Mandiant experts conduct a series of onsite workshops in collaboration with key stakeholders from the client organization to perform data collection and script output analysis based on existing technologies and processes. Our experts use this information to evaluate the architecture (including both on-premise and cloud-based environments) and identify possible attack paths within the Active Directory infrastructure.

Mandiant consultants recommend ways to harden privileged user access and privileged access management, enhance visibility and detection of malicious events within Active Directory and provide a strategic roadmap of recommendations to improve the overall security posture of the client's Active Directory infrastructure.

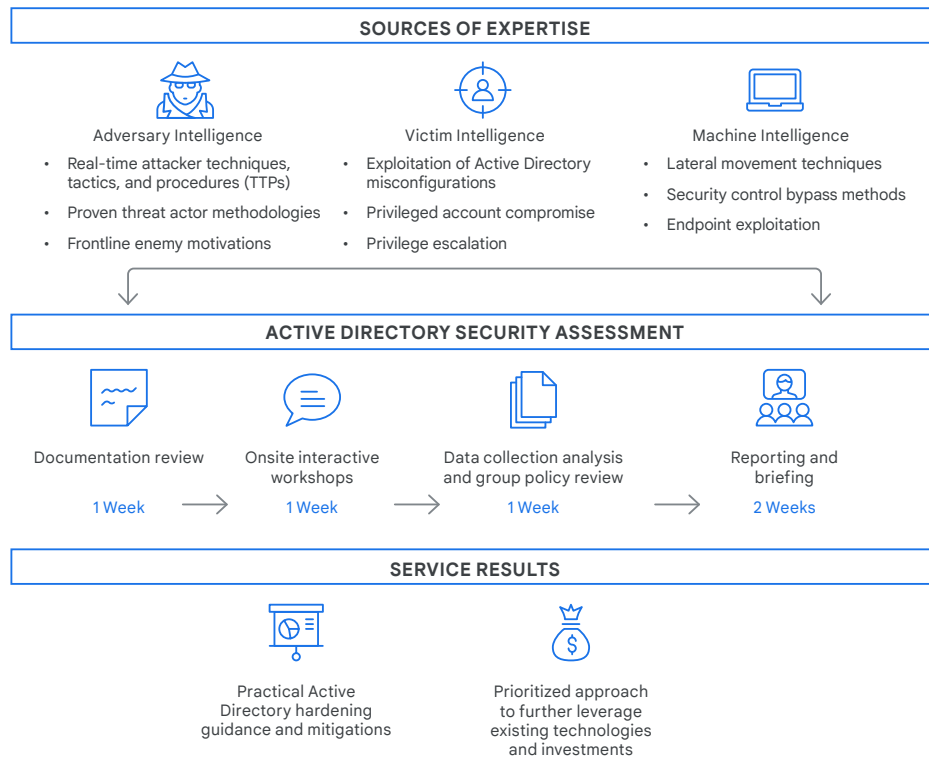


Figure 1. Service lifecycle.

Benefits:

- Forest architecture and trusts
- Operational processes
- Monitoring and response
- Privileged accounts and access management
- Group policy controls and enforcement
- Permission delegation
- Service accounts and service principal names (SPNs)
- Remote access controls and hardening
- Endpoint configuration and hardening
- Integration with Microsoft Azure and Microsoft Office 365

Deliverables

The assessment concludes with a detailed report that includes:

- A snapshot of the existing Active Directory security configuration for the environment
- Specific Active Directory security best practices to align with current technologies and operational processes
- Practical recommendations for restricting, managing, and monitoring privileged user access and accounts within the environment
- Detailed recommendations for further hardening the security posture of the Active Directory infrastructure