semperis

Active Directory Architecture Review

Enterprise organizations with legacy Active Directory (AD) infrastructures often struggle to implement and maintain optimal AD security operations because of underlying AD architecture challenges. As companies grow, acquire other companies, and reorganize business units, the identity environment can degrade, accumulating misconfigurations and opening security vulnerabilities that threat actors can exploit.

An Active Directory Architecture Review, guided by Semperis identity experts, provides a thorough review of the current AD environment, identifies opportunities to improve security and operations practices, and provides review sessions and tools to empower IT and security teams to maintain best practices going forward.

Expert-guided Active Directory Architecture Review

The Active Directory (AD) Architecture Review is a structured evaluation of the AD environment to ensure it is secure, efficient, and aligned with best practices. This process involves collecting and analyzing information about various aspects of the AD infrastructure, interviewing stakeholders, and comparing the current state to industry standards and future goals.

AD environment information gathering

To start the architecture review process, Semperis experts collect detailed information on each component of the AD environment, including:

- Documenting the structure and relationships between domains and forests
- Mapping the DNS zones, records, and their integration with AD
- Conducting an inventory and evaluation of domain controllers, Active Directory Federation Services (ADFS), Active Directory Certificate Services (ADCS), Active Directory Rights Management Services (ADRMS), and multi-factor authentication (MFA)
- Assessing other factors of the AD environment, including the organizational unit layout, GPO design, user account inventory, token sizes, and more
- Reviewing backup strategy, current performance levels, integration with cloud identity providers, and more

Interviews to assess current and future AD operation needs

Next, the Semperis team gathers insights from the administration team about the AD environment's operation, issues, and future needs, including:

- Current functional and security requirements for each component of the AD environment, required compliance with industry standards, and future AD environment requirements and goals
- Current AD governance practices, AD monitoring and management tools, AD backup and recovery procedures, GPO management, patching processes, and service account lifecycle management
- AD environment collaborators, including AD administrators, IT managers, security team members, compliance officers, and leaders

> “Nearly half of Microsoft incident response engagements involved insecure AD configurations.”
>
> **Microsoft Digital Defense Report**

Remediation planning, knowledge transfer, and documentation

Following the information gathering and review sessions, the Semperis team will:

- **Develop a detailed plan** to remediate identified issues and improve the AD environment
- **Conduct knowledge transfer sessions** to equip the AD team for maintaining sound AD security practices
- **Provide detailed documentation** about AD configurations, change management logs, incident response plans, operational procedures, disaster recovery plans, and security policies.

Active Directory Architecture Review outcomes

- Inventory and documentation of AD environment components and areas for review or improvement
- Detailed insights into the AD environment’s operational challenges and requirements, governance procedures, and opportunities for improvement
- Comprehensive assessment report on the AD environment architecture and health
- Detailed remediation plan with timelines and responsibilities
- Comprehensive documentation that supports ongoing AD security best practices, management, and compliance

Unmatched global identity forensics and incident recovery experience

To learn more about Semperis Active Directory Architecture Review services, visit **Semperis.com**

90+	years' identity-related incident response experience
170+	combined years of Microsoft MVP experience
25+	former Microsoft Premier Field Engineer (PFEs) on staff
30+	years' data analysis for insider threat & risk monitoring

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

Gartner Peer Insights. Customer First

Semperis
IT Resilience Orchestration
5.0
Source: Gartner Peer Insights

Leader SPRING 2024

Semperis
Directory Services Protector
4.7
Source: G2.com

Semperis Headquarters
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030