

Active Directory Security Assessment

Secure the foundation of your kingdom

Active Directory (AD) is one of the pillars of Identity and Access Management (IAM), providing authentication and authorization protocols for on-premises systems and integrated cloud platforms. As such, AD holds the “keys to the kingdom.” If attackers compromise your AD environment, they can move laterally to business-critical systems—which makes AD a prime target.

The Semperis Active Directory Security Assessment (ADSA) provides an accurate view of the strengths and weaknesses in your current AD environment—with emphasis on protecting Tier 0 assets—and creates a documented set of recommendations for improving security tailored to your environment.

Performing an Active Directory security assessment is essential

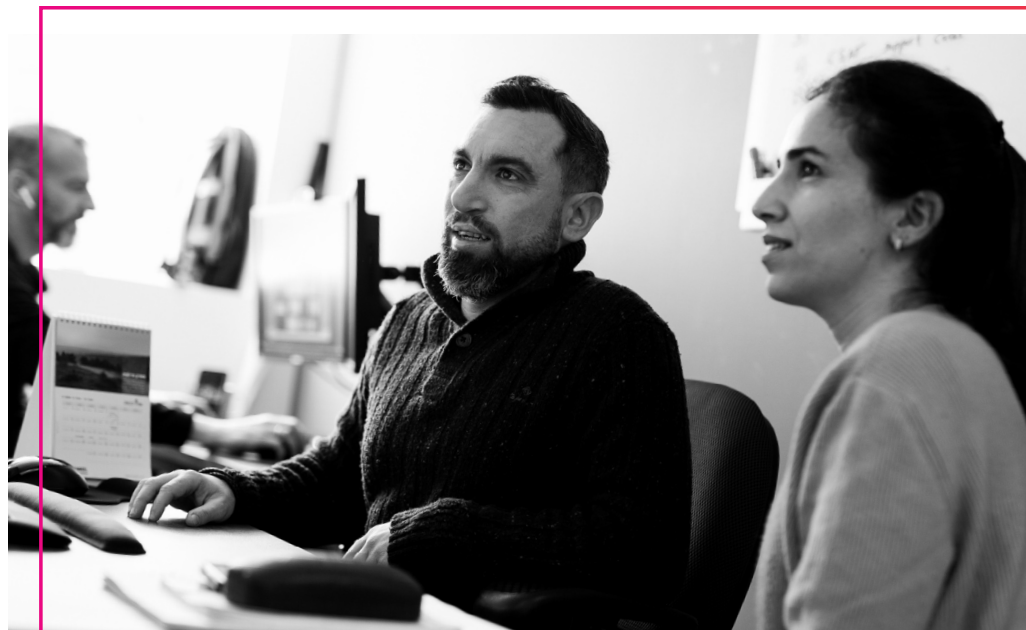
Active Directory is the foundation of the IAM infrastructure that authenticates users and grants access to resources and integrated systems. Once an attacker compromises AD, they can abuse it to gain access to the business-critical systems directly or indirectly controlled by AD.

Active Directory is a complex system with numerous configurable settings and features, making it hard to secure. Design flaws, operational mistakes, and misconfigurations accumulate over the years to create a technical debt that is difficult to address. This technical debt exposes AD to attacks of varying levels of sophistication, making AD the path of least resistance for an attacker to reach critical systems and sensitive data.

The Semperis Active Directory Security Assessment—developed by Semperis AD and security experts—gives the organization a clear picture of their AD security posture and a roadmap to address the exposures found at the strategic, operational, and tactical levels. Our team can conduct the Active Directory Security Assessment in preparation for a potential breach to minimize its impact or post-breach to contain and eradicate an active threat.

KEY BENEFITS





- Reviews architectural, operational, and technical levels through a comprehensive assessment
- Aligns with industry best practices and hinders adversary tactics, techniques, and procedures (TTP)
- Produces an actionable roadmap geared toward reaching the desired state
- Provides a strategic roadmap for improving security posture and tactical steps for mitigating security exposures



How Semperis strengthens your defenses

The Active Directory Security Assessment is conducted by Semperis' team of AD security professionals through a combination of technical and non-technical engagements. We use questionnaires and interviews to elicit architectural and operational information from your organization's key personnel. We also use automated scans and manual tools to collect technical information from AD and auxiliary systems.

The assessment comprises the following efforts:

-  Security architecture review
-  Operational procedures review
-  Security configuration review
-  Attack paths analysis

Our team analyzes the data captured in the assessment to produce details that depict the current state and an actionable roadmap for bringing the AD environment to an achievable, secure state. The team also conducts interviews to understand your operational procedures and provide recommendations for improvement.

Action plan and security roadmap

The Active Directory Security Assessment produces a detailed list of findings, each with a concise description of the identified issue, the risk it imposes, a severity rating to support prioritization, and guidelines for remediation.

The report presents a depiction of the current state of the AD environment with the key exposures identified. The report provides details to achieve an improved state through a set of efforts to improve the security posture of AD. Each finding provides the detail, impact, recommendations, and references to address the exposure. The detailed report helps you build a tactical course of action to strengthen your defenses against attacks that target Active Directory.



Semperis helped us understand the different phases of the attack and possible future attacks, and helped detect and **shut down the hackers** once they got in. Semperis knows exactly what to look for and has the tools to do it.

► CTO of large orthopedic practice that engaged Semperis for post-breach assessment and recovery



info@semperis.com
www.semperis.com

Semperis Headquarters
221 River Street
9th Floor
Hoboken, NJ 07030