

SERVICE DATA SHEET

Active Directory Security

Find the attack paths to domain admin before an intruder does

Active Directory controls who can access almost everything in a Windows network. That makes it a prime target for ransomware operators: once an attacker controls the domain, they control your servers, workstations and data.

Years of growth leave most directories with stale accounts, excessive privileges, weak service account passwords and misconfigured delegation. Each is a small issue on its own. Chained together, they can give an ordinary user a path to domain admin in hours.

SentryArk's Active Directory assessment finds those paths and shows you how to close them, combining configuration review with the hands-on techniques real threat actors use.

CONFIGURATION REVIEW AND ATTACK PATHS

We analyse your directory's users, groups, permissions, trusts and Group Policy to map every route from a standard account to your most privileged ones. Each path is verified by hand, so you get real risks rather than a list of theoretical warnings.

- Privileged groups and ACLs
- Kerberoasting and AS-REP roasting
- Delegation and trust abuse
- Group Policy and LAPS
- AD CS certificate abuse
- Password policy and hygiene

ASSUMED BREACH TESTING

Most intrusions start with a single compromised laptop. We start from the same position, a standard domain user on a standard workstation, and attempt credential theft, privilege escalation and lateral movement as an attacker would, under agreed rules of engagement.

Hybrid environments are covered too, including Entra ID synchronisation and the paths that let an on-premises compromise reach your cloud tenant.

ASSESSMENT DETAILS AND METHODOLOGY

Our methodology combines automated attack path mapping with manual exploitation, aligned with MITRE ATT&CK. Every action is logged, so your team can check what was detected.

Planning and scoping	01	We agree the domains, forests and trusts in scope, the starting accounts and any systems that must not be touched.
Enumeration	02	We collect users, groups, ACLs, Group Policy, trusts and certificate templates, and map attack paths to tier-zero assets.
Vulnerability analysis	03	We review configuration against Microsoft and CIS hardening guidance and flag weak passwords, stale objects and risky delegation.
Exploitation and escalation	04	We safely verify the most critical paths through credential attacks, delegation abuse and lateral movement towards domain-level control.
Reporting	05	Attack path diagrams, prioritised fixes and quick wins that remove the most risk for the least effort.

The assessment includes

- Executive summary
- Misconfigurations with risk ratings
- Prioritised hardening roadmap
- Attack path diagrams to tier-zero assets
- Credential and password hygiene findings
- Detection recommendations for your SOC

ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.