ON-PREMISES IDENTITY SECURITY

# Active Directory security audit.

Understand the identity and configuration exposure in your on-premises environment. Connect directory, host and policy evidence to practical hardening work.

## HOW IT WORKS

1. **Confirm the collection host and permissions.**
   Agree the domains, the approved Windows collection host and the modules and access the audit needs.
2. **Collect directory, policy and host evidence.**
   Gather the available directory, privileged-group, Group Policy, certificate-services and host-configuration sections.
3. **Analyse identity and configuration exposure.**
   Review privileged access, delegation, password policy, certificate templates and domain-controller hardening together.
4. **Prioritise with the administrator.**
   Turn findings into hardening work, naming the affected accounts, policies or hosts and their service dependencies.
5. **Re-collect for follow-up.**
   After authorised changes, run a later collection to provide evidence for the next review.

## CONDITIONS AN ACTIVE DIRECTORY AUDIT CAN SURFACE

- Over-privileged, stale or duplicate accounts, and unexpected membership of privileged groups.
- Risky delegation and directory access-control settings.
- Weak or inconsistent password-policy configuration.
- Group Policy and SYSVOL exposure that needs review.
- Active Directory Certificate Services templates configured in a way that widens exposure.
- Domain-controller hardening, supported-protocol and patching gaps.

*An exposed permission or certificate-template configuration is a posture finding, not proof that an attacker used it. Confirming a suspected compromise needs activity evidence and further investigation.*

**Framework alignment.** Active Directory findings can be discussed against CIS-aligned hardening references and NIST Cyber Security Framework perspectives, and they help evidence the access-control and secure-configuration themes behind a UK Cyber Essentials review of your on-premises estate.

## Start with an authorised, read-only scope

Begin with your assessment questions; we agree coverage and delivery before any commitment.

**threatshield@threatshield.global**
**Read the full page ↗**

ThreatShield is part of ITS Consulting — ITS Consulting Ltd (United Kingdom) and ITS Consulting LLC (United States). This guide summarises an assessment capability; the actual scope, coverage and evidence available depend on your environment, licensing and permissions. Framework references organise findings and are not a certification or an assurance that a control is effective. © 2026 ThreatShield.