SafeLink IT
Mehr als nur Sicherheit

FICTIONAL SAMPLE - NO REAL CLIENT DATA

AD HARDENING SNAPSHOT

Sample Report

A fictional but realistic sample showing how messy Active Directory risk becomes a clear, prioritized hardening roadmap - without breaking operations.

Tier 0 | Privileged Access | AD CS | Domain Controllers | 90-Day Roadmap

Focus areas

- Tier-0 boundary and ownership
- Privileged access cleanup
- AD CS authentication risk
- Domain Controller protection
- Legacy authentication reduction
- 30/60/90-day roadmap

PREPARED FOR

Asteron AG

Fictional organization used only for this sample report.

DOCUMENT

Sample v1.1 | 19 May 2026

Read-only assessment style. No exploitation. No real client data.

Overall posture: elevated AD takeover risk

Asteron's Active Directory is operationally mature, but several control-plane boundaries are porous. The key issue is the combination of inherited Tier-0 access, certificate-based authentication risk, and privileged account usage from normal endpoints.

AD SCORE

68

/ 100

Elevated risk: prioritize Tier 0, AD CS, and privileged logon paths before broader modernization.

TOP BUSINESS RISK

A compromised admin workstation or over-permissioned service account could become a path toward domain control.

TOP TECHNICAL RISK

Two certificate templates allow authentication-related enrollment conditions outside the intended privileged-access boundary.

23

INDIRECT TIER-0 PRINCIPALS
via nesting or delegated paths

18

PRIVILEGED LOGONS FROM STANDARD ENDPOINTS
observed in sample telemetry

2

RISKY CERTIFICATE TEMPLATES
authentication-impacting templates

3

LEGACY DELEGATION SYSTEMS
require migration planning

Scope and assessment method

In scope

FOREST	corp.asteron.example
DOMAINS	corp, emea, legacy
USERS / GROUPS	Approx. 4,800 users, 1,260 groups
SERVERS	Approx. 420 Windows servers
DOMAIN CONTROLLERS	13 DCs across 4 sites
AD CS	2 enterprise CAs, 47 templates

Data reviewed

- AD users, groups, ACLs, delegation attributes, and nested memberships.
- Privileged group memberships and admin account usage patterns.
- Certificate Authority and certificate template configuration export.
- GPO reports for DCs, admin workstations, and privileged accounts.
- Sample logon telemetry and owner interviews.

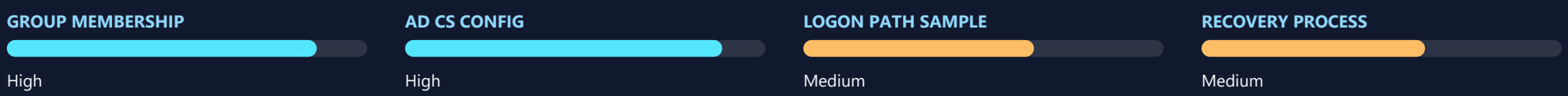
Out of scope

Endpoint forensics, malware hunting, password guessing, live exploitation, production changes, Entra ID conditional access, and network scanning outside the approved asset list.

Safety principle

Read-only wherever possible. Findings are validated through configuration evidence, owner interviews, and safe query results - not exploitation.

Report confidence



25-question scorecard condensed into ten areas

Scoring is illustrative. It shows how a technical review becomes a management-readable risk picture.

Tier-0 boundary and ownership

56

Elevated risk

Admin workstations and logon paths

58

Elevated risk

Privileged groups and service accounts

64

Needs cleanup

AD CS templates and CA governance

42

High priority

Domain Controller protection

74

Partially mature

Delegation and lateral movement paths

57

Needs triage

Legacy authentication exposure

63

Stage changes

Backup and forest recovery

63

Untested plan

Governance and recertification

66

Owner gaps

Operational change readiness

78

Good foundation

What the score means

0-25	Critical control-plane exposure. Stabilize immediately.
26-50	High risk. Remove unsafe paths before broader modernization.
51-75	Elevated risk. Prioritize cleanup and governance.
76-90	Good. Maintain with monitoring and recertification.
91-100	Strong. Continue evidence-based assurance.

Interpretation

AD is not judged by the number of settings changed. It is judged by whether the control plane is clear, protected, recoverable, and administrable by real IT teams under pressure.

Risk is concentrated around control-plane paths

Legend

Rows represent business impact. Columns represent likelihood based on exposure, path complexity, telemetry confidence, and operational feasibility. This sample avoids exploitation details.

- F01 — Tier-0 inherited control
- F02 — AD CS unsafe template
- F03 — Privileged logon paths
- F04 — Unconstrained delegation
- F05 — LDAP / legacy auth exposure

Prioritized findings

ID	FINDING	SEVERITY	AFFECTED	IMPACT	PRIORITY
F01	Indirect Tier-0 control through nested admin paths	Critical	23 principals	Domain control path	0-15 days
F02	AD CS unsafe authentication template	Critical	2 templates	Privileged identity risk	0-7 days
F03	Privileged logons from standard workstations	High	18 accounts	Credential theft exposure	0-30 days
F04	Unconstrained delegation remains on legacy servers	High	3 servers	Lateral movement risk	0-30 days
F05	LDAP signing / channel binding not enforced	High	Domain-wide	Relay and downgrade risk	30-60 days
F06	Long-lived privileged service accounts	Medium	7 accounts	Credential reuse / blast radius	30-90 days
F07	Domain Controller admin exceptions too broad	Medium	2 GPOs	Tier-0 exposure	30-60 days
F08	Forest recovery process not tested	Medium	Process	Recovery uncertainty	30-90 days
F09	Privileged group nesting lacks owner review	Medium	14 groups	Governance drift	30-60 days
F10	Legacy Kerberos / NTLM dependencies	Medium	39 accounts / apps	Downgrade exposure	30-90 days

Indirect Tier-0 control through nested admin paths

Several non-Tier-0 admin groups currently gain effective control over Domain Controller administration through nested memberships and delegated rights.

Synthetic evidence highlights

- CORP\Server-Admins-Legacy -> CORP\Backup-Operators-Domain -> DC administration path.
- 23 direct or indirect principals on Tier-0-equivalent paths.
- 6 shared or service identities found in privileged nesting.
- 4 privileged paths without an assigned owner.

CRITICAL

Why it matters

If a non-Tier-0 admin account or legacy management server is compromised, the attacker may inherit enough access to administer Domain Controllers or weaken recovery.

OWNER

Infrastructure / Identity Platform

TARGET STATE

Tier-0 administration is explicit, minimal, owned, reviewed, and restricted to hardened administrative paths.

Immediate actions

- Freeze new membership changes on identified Tier-0-equivalent groups.
- Remove non-Tier-0 groups after impact review.
- Create an exception register with owners and expiry dates.

Strategic controls

- Separate daily, server-admin, and Tier-0 personas.
- Allow Tier-0 accounts only from approved admin paths.
- Track Tier-0-equivalent principal count as a metric.

AD CS authentication template does not match trust boundary

Certificate Services can grant identity trust. Two templates reviewed in this sample allow conditions that are too broad for authentication-capable certificates.

Synthetic template evidence

- Template: UserSmartcard-Compat.
- Purpose: Client Authentication.
- Enrollment includes broad operational groups.
- Requester-controlled subject behavior requires review.

CRITICAL

Why it matters

Certificate-based authentication can bypass normal password lifecycle assumptions. Identity risk can persist after password resets and group cleanup.

OWNER

Identity Platform / PKI owner

TARGET STATE

Authentication-capable templates have explicit scope, approval where needed, and monitoring for privileged identity issuance.

Immediate actions

- Disable unused risky templates or restrict enrollment.
- Identify active consumers and rollback options.
- Separate admin-use templates from user workflows.

Strategic controls

- Monthly template and CA permission review.
- Certificate issuance monitoring for privileged identities.
- Documented owner for every authentication template.

Privileged identities are usable, but not yet trustworthy under pressure

Observed patterns

- 18 privileged accounts observed logging on from standard or shared admin workstations.
- 7 privileged service accounts have stale password age or unclear rotation ownership.
- 14 privileged groups do not have a named owner in the reviewed inventory.
- Emergency Domain Admin procedure exists, but checkout evidence is inconsistent.

Desired state

- Privileged accounts are separate from daily user accounts.
- Tier-0 accounts are used only from approved administrative paths.
- Service accounts have owner, purpose, rotation strategy, and minimum rights.
- Privileged membership is reviewed with evidence, not memory.

12

DOMAIN ADMINS
Target: 4-6 named plus break glass

3

ENTERPRISE ADMINS
Target: empty by default

7

PRIVILEGED SERVICE ACCOUNTS
Need owner and rotation

14

OWNERLESS PRIVILEGED GROUPS
Governance drift

Pragmatic first step

Create a privileged-access inventory with three columns only: account/group, owner, and reason. Anything without an owner or reason becomes a cleanup candidate, not an automatic deletion.

Change caution

Service accounts often hide business dependencies. Remediation should use test windows, application owner sign-off, and rollback-ready changes.

Domain Controller hardening is partially mature; legacy paths need staged reduction

Domain Controllers

- Baseline GPOs exist and are mostly consistent across DC OUs.
- Two administrative exception groups can log on more broadly than required.
- Patch workflow exists, but DC-specific ring testing is informal.
- Backup exists, but a full forest recovery exercise was not evidenced in the last 12 months.

Authentication and delegation

- 3 legacy servers retain unconstrained delegation due to historical application design.
- LDAP signing and channel binding enforcement is inconsistent.
- 39 accounts or applications show dependency signals for NTLM or legacy Kerberos crypto.
- Audit data is enough for planning, but not yet enough for strict enforcement.

Recommended hardening sequence

1	Remove broad DC interactive logon exceptions after owner review.	**Low disruption**
2	Replace unconstrained delegation with safer application-specific patterns.	**Medium disruption**
3	Audit NTLM, LDAP signing, channel binding, and legacy crypto dependencies.	**Low disruption**
4	Enforce in test, pilot, then production waves with rollback criteria.	**Controlled disruption**

A practical hardening roadmap that IT can actually run

Tier-0-equivalent principals	Risky auth templates	Privileged logons from standard endpoints	Forest recovery test date
23 -> target 8-12	2 -> target 0	18 -> target 0	Unknown -> scheduled

0

Days 0-15

Stabilize control plane

- Disable or restrict risky certificate templates.
- Freeze and review Tier-0-equivalent group changes.
- Assign owners to privileged groups.
- Define emergency admin evidence.

30

Days 16-30

Clean admin paths

- Remove non-Tier-0 groups from DC admin paths.
- Pilot privileged admin workstation policy.
- Review service account purpose and rights.
- Create exception register and expiry dates.

60

Days 31-60

Reduce legacy exposure

- Audit NTLM, LDAP signing, channel binding, and legacy Kerberos crypto.
- Plan delegation migration for legacy systems.
- Start gMSA migration for eligible services.
- Implement membership recertification.

90

Days 61-90

Make it sustainable

- Run forest recovery tabletop or lab restore.
- Publish Tier-0 dashboard.
- Enforce staged authentication hardening.
- Schedule quarterly AD hardening review.

What a client receives after the AD Hardening Snapshot

Deliverables

- Executive risk summary in business-readable language.
- Technical finding register with evidence, owners, and priority.
- Tier-0 exposure overview and privileged path cleanup recommendations.
- AD CS risk notes with template and CA governance recommendations.
- 30/60/90-day remediation roadmap for real IT teams.

Typical inputs needed

- Read-only AD export or approved assessment account.
- GPO reports for DCs, privileged accounts, and admin workstation policies.
- Certificate template and CA configuration export.
- Privileged group inventory and known exception list.
- One workshop with identity, infrastructure, and security owners.

Safety boundaries

- No surprise changes.
- No password guessing.
- No exploitation of certificate or delegation findings.
- No production change without written approval, owner sign-off, and rollback plan.

Best next conversation

Bring one AD concern, audit comment, or pentest finding to a 30-minute Teams call. The goal is simple: leave with a clearer, safer next step.

ASSESSMENT FOCUS

Turn messy Active Directory risk into a clear, prioritized hardening roadmap - especially around Tier 0, privileged access, AD CS, and Domain Controller protection.

Example evidence extracts

Privileged group nesting

Group: CORP\Backup-Operators-Domain
Owner: Missing
Reason: Legacy backup platform
Path: DC local admin via GPO exception
Recommendation: split backup role from DC admin rights

Service account review

Account: CORP\svc_legacy_deploy
Last password set: 491 days
Privileged groups: Server-Admins-Legacy
Interactive logon: not restricted
Recommendation: assign owner, restrict logon, migrate to gMSA where feasible

Domain Controller policy sample

GPO: DC-Baseline-2024
Audit policy: present
Local admin exception: present
Interactive logon allowed: Domain Admins, DC-Operations, backup exception group
Recommendation: remove non-Tier-0 groups after impact review

AD CS template sample

Template: UserSmartcard-Compat
EKU: Client Authentication
Subject supply: requester-supplied
Enrollment group: broad
Manager approval: disabled
Recommendation: restrict enrollment and review subject behavior

Evidence policy

A real report includes enough evidence for the client to reproduce and remediate the finding, while avoiding unnecessary exposure of sensitive object names, SIDs, certificates, or administrative paths.

Defensive basis

This is not a compliance report. The references below support the defensive themes used in the sample: excessive privilege reduction, secure administrative hosts, Tier-0 thinking, Domain Controller protection, AD CS hardening, and AD compromise mitigation.

Reference	Why it matters for this sample
Microsoft - Best practices for securing Active Directory	Least-privilege administration, secure admin hosts, and Domain Controller protection.
Microsoft - Securing privileged access: Enterprise access model	Tier-0 and privileged-access boundary framing.
Microsoft - Securing Domain Controllers against attack	Domain Controller hardening and baseline recommendations.
Microsoft Tech Community - Secure configuration and hardening of AD CS	AD CS review theme and certificate services as identity infrastructure.
ASD's ACSC and partners - Detecting and mitigating AD compromises	Common AD compromise paths and pragmatic mitigation strategies.

End of sample report

Calm AD hardening for serious Microsoft environments.