

Identity Exposure Review

Which paths lead from an ordinary account to control of Active Directory and Entra ID, and which of your credentials are already exposed.

The question it answers

How far could someone get with one ordinary account? Active Directory and Entra ID are assessed as one attack surface, together with the trust between them, and every path to the Tier 0 assets is traced with the configuration that opens it.

The principal consultant also researches leaked and exposed credentials belonging to the organization, so each exposed account is read against the paths it would open.

Read and validate

The review starts from read-only directory access or a standard-user foothold. Directory objects are not changed, and denial of service is excluded.

The most significant paths are validated by controlled exploitation only where that is agreed in writing, so every reported path carries evidence of real impact.

What the review covers

Tiering and privileged access

How administrative accounts and tiers are separated, and the paths that cross those boundaries.

Delegation and certificate services

Kerberos delegation, and certificate templates and permissions in Active Directory Certificate Services that could give an ordinary account privileged access.

Hygiene, protocols, groups and trusts

Credential practices, legacy authentication protocols, nested groups, and trusts between forests and between Active Directory and Entra ID.

Exposed credentials

Credentials tied to the domains in scope, researched by the principal consultant and read against the mapped paths.

AT A GLANCE

APPLIES TO

Active Directory, Entra ID and the trust between them

STARTING POINT

Read-only access or a standard-user foothold

DURATION

1 to 5 weeks for the directory assessment

MAPPING

MITRE ATT&CK, for hardening and detection

DELIVERY

Principal consultant, start to finish

WHO THIS IS FOR

- Organizations that want the routes to domain and tenant control found and closed first.
- Hybrid estates where Active Directory and Entra ID have not been assessed as one surface.
- SOC teams that need to know which identity attacks to detect.
- Directory teams that need a sequenced hardening plan.

How a review runs

01**Preparation and access**

Scope, rules of engagement and the starting access are agreed in writing.

02**Collection and research**

Users, groups, privileges, trusts and certificate templates are enumerated, and the credential research for the domains in scope runs in the same phase.

03**Analysis**

Privilege relationships, tiering, delegation, certificate templates, credential exposure and legacy protocols are analyzed, and viable paths are mapped.

04**Validation**

The most significant paths are validated by controlled exploitation, within agreed limits.

05**Report and debrief**

Attack paths, root causes and prioritized remediation are walked through with the directory and identity teams.

WHY ALEXSTA

- The paths and the exposed credentials are reported together, so priorities follow real exposure.
- Every path comes with its evidence and its root cause, not a score.
- ATT&CK mapping turns each finding into a hardening change and a detection priority.

WHAT IS NEEDED TO SCOPE IT

- Active Directory domains and forests, with approximate user and computer counts.
- Whether Entra ID and hybrid identity are in scope.
- Whether certificate services are deployed and in scope.
- Starting position, and the domains whose credentials are researched.

What you receive

Assessment report

Findings with evidence, severity, attack-path narratives and root causes, with an executive summary.

Hardening roadmap and exposed credentials

Sequenced changes that close the paths, and the exposed accounts read against them.

Attack-path diagrams

The privilege-escalation routes identified, drawn out.

Detection recommendations

ATT&CK-mapped guidance on the identity attacks the SOC should detect.

Request an engagement

Share how many domains and tenants you run and whether certificate services are deployed, and the review can be scoped in one call.

contact@alexsta-cybersecurity.com

+41 76 76 44884

alexsta-cybersecurity.com