eSurelTy

ENTRA ID PENETRATION TESTING & ACTIVE DIRECTORY AUDIT

Fortify your identity infrastructure before it becomes the easiest path to business disruption.

Identity Failures Now Create Coverage Risk

Attackers monetize identity and access management mistakes. Misconfigured Entra ID and legacy Active Directory expand ransomware blast radius, create silent privilege creep, and expose gaps auditors and boards no longer ignore.

eSurelTy tests your actual exposure, shows how compromise would propagate across Entra ID and AD, and gives you the shortest path to a hardened, defensible identity stack.

Where Identity Programs Actually Break

Most breaches start with compromised credentials or broken identity.

Common breakdowns:

- Active Directory Domain Misconfigurations — Stale accounts, weak or conflicting GPOs, legacy trusts, replication blind spots, unpatched domain controllers.
- Entra ID Security Gaps — Weak MFA enforcement, over-broad admin roles, brittle Conditional Access, risky app consents, unmanaged third-party integrations.
- Privilege Overprovisioning — Local admin inheritance, shadow admin accounts, “temporary” elevated access that becomes permanent, lack of JIT/JEA.
- Hybrid trust weaknesses — Mis-scoped federation, token replay paths, on-prem to cloud escalation, exposed sync accounts, incomplete break-glass strategies.
- Governance Gaps — No defensible IAM maturity model, missing ownership and exception handling, weak access review cycles, inconsistent joiner/mover/leaver flows.

Consequence: higher breach likelihood, higher loss severity, and documentation gaps insurers use to limit payout.

Non-Negotiables for Modern IAM

eSurelTy audits and tests identity against a small set of non-negotiables:

- Enforced MFA and risk-based access for all privileged roles
- Least-privilege by design, with provable removal of standing admin rights
- Conditional Access that cannot be bypassed by legacy protocols or token reuse
- Hardened AD trusts, GPOs, and tiered admin model with workstation segregation
- Hybrid identity configuration that resists on-prem ↔ cloud pivoting
- Evidence: controls, logs, and procedures that stand up to technical and governance scrutiny

Contact Us

info@eSurelTy.com

www.eSurelTy.com

Threat-led assessment approach

Threat-led. Insurance-aligned. Outcome-driven.

Phase 1 — Discovery & Mapping

- Enumerate forests, domains, trusts, Entra tenants, apps, and service principals
- Surface misconfigurations, policy drift, and privilege escalation paths
- Build an attack graph showing how compromise would actually spread across Entra ID and AD

Phase 2 — Penetration Testing & Risk Scoring

- Execute real-world IAM attack chains across AD and Entra ID
- Validate bypasses of MFA, Conditional Access, and role boundaries
- Quantify risk with impact-based scoring tied to business-critical loss drivers

Phase 3 — Governance & Maturity Review

- Rate identity governance against a CMMI-inspired maturity model
- Map controls to NIST 800-53 / ISO 27001 expectations
- Produce a prioritized roadmap that raises both security posture and operational discipline

Testing & Audit Scope

- Active Directory audit: Domain health, GPO hygiene, replication status, privileged and stale identities, trust relationships.
- Entra ID penetration test: MFA enforcement, Conditional Access policies, consented apps, role assignments, token handling, risky legacy protocols.
- Hybrid trust evaluation: Federation and sync configuration, token flows, break-glass accounts, pivot paths between on-prem and cloud.
- Workstation privilege review: Local admin inheritance, elevation paths, endpoint hardening gaps, workstation-tier alignment with AD controls.
- IAM risk quantification: Prioritized scoring and an evidence pack that links findings to concrete attack paths and business impact.

Deliverables built for security and governance

Executive report + dashboard

Ranked findings with business impact, attack-path visuals, and a clear remediation plan.

Governance and maturity scorecard

Ratings across policies, provisioning, password standards, and access reviews with NIST/ISO mapping.

Risk remediation roadmap

Stepwise actions for MFA enforcement, privilege reduction, trust hardening, and Conditional Access fixes with owners and timelines.

Why eSurelTy

- ✓ IEvidence-aligned from the start: artifacts and scoring designed for senior leadership, auditors, and third-party reviewers
- ✓ Certified IAM specialists on every engagement: CISSP, CISA, CEH, and Azure credentials
- ✓ Hybrid identity depth: Entra ID and on-prem AD treated as a single attack surface, not separate silos
- ✓ Proof over promises: exploit-validated findings, not theoretical misconfiguration lists
- ✓ From audit to improvement: prescriptive, realistic fixes that can be implemented and verified

Strengthen identity before the next credential is abused.

Schedule your Entra ID Penetration Testing & Active Directory Audit with eSurelTy.

Contact Us

info@eSurelTy.com

www.eSurelTy.com