

TECHNICAL PRODUCT BRIEF

Active Directory and identity penetration testing

Expose the identity paths that lead to privileged control.

Why customers use this service

Review and test representative Active Directory access to identify credential, delegation, permission and trust paths that could expand one account into wider administrative control.

What we assess

Identity exposure	Users, groups, computers and services visible to an attacker.
Credential paths	Weak, reusable or recoverable credential material.
Permission chains	ACLs, group membership and delegated rights that enable escalation.
Service accounts	Privileges, configuration and authentication risks around services.
Administrative tiers	Separation between ordinary, server and domain administration.
Domain and forest trusts	Paths that cross identity or organisational boundaries.
Policy and hardening	Controls that reduce common identity attack techniques.

Engagement outcome

An identity attack-path report with validated evidence, affected principals, prioritised remediation and retest results.

How the engagement works

How we test or review

Damocles analyses directory identities, groups, ACLs, delegation, trusts, credentials and sessions from the supplied foothold, validating only the minimum safe step needed to prove a privilege path. Directory exports support but do not replace live evidence; protected accounts and disruptive credential activity remain excluded.

Testing and review perspectives

Assumed internal foothold

Queries authorised directory and host information from the supplied compromise position.

Included when: Used to identify relationships and opportunities available before a domain identity is supplied.

Access: A controlled internal host or connection, scope boundaries and approved directory endpoints.

Limitations: Represents one foothold and does not imply access from every segment or host.

Standard domain user or workstation

Uses a dedicated domain user and representative workstation to inspect groups, credentials, delegation, sessions and reachable administration paths.

Included when: Used for identity and privilege behaviour available to an ordinary principal.

Access: A test user, workstation context, domain scope and protected-account exclusions.

Limitations: Findings apply to the supplied group membership, workstation and current directory state.

Directory privilege-path reviewer

Analyses group nesting, ACLs, delegation, service accounts, trusts, certificate services and administrative relationships to construct privilege paths.

Included when: Used where directory evidence can substantiate escalation or tier-boundary findings.

Access: Authorised directory queries or exports, representative identities and system ownership data.

Limitations: Does not imply every domain object or privileged relationship was validated.

Customer access or evidence typically required

A controlled internal host or connection, scope boundaries and approved directory endpoints.; A test user, workstation context, domain scope and protected-account exclusions.; Authorised directory queries or exports, representative identities and system ownership data.

What you receive

An identity attack-path report with validated evidence, affected principals, prioritised remediation and retest results.

Detailed technical coverage

Supplied starting identity

What is assessed	Damocles records the supplied identity, workstation, network position, group membership and expected trust context before directory queries begin.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for supplied starting identity.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to supplied starting identity.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Supplied starting identity when the directory relationship or authorised system is present in scope.
Limitations	The conclusion is limited to the sampled supplied starting identity; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.

Users and groups

What is assessed	Damocles enumerates authorised users, groups, nesting, privileged membership and directory ACLs to identify unexpected identity relationships.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for users and groups.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to users and groups.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Users and groups when the directory relationship or authorised system is present in scope.
Limitations	The conclusion is limited to the sampled users and groups; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.

Service accounts

What is assessed	Damocles examines service-account privilege, delegation, logon rights, credential handling, ownership and lifecycle evidence.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for service accounts.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to service accounts.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Service accounts when the directory relationship or authorised system is present in scope.
Limitations	The conclusion is limited to the sampled service accounts; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.

Credential exposure

What is assessed	Damocles inspects authorised hosts, shares, directory attributes, scripts and configuration for exposed or reusable credential material without bulk harvesting.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for credential exposure.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to credential exposure.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Credential exposure when the directory relationship or authorised system is present in scope.
Limitations	The conclusion is limited to the sampled credential exposure; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.

Delegation

What is assessed	Damocles analyses constrained, unconstrained and resource-based delegation and validates only the minimum safe identity transition needed to prove risk.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for delegation.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to delegation.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Delegation when the directory relationship or authorised system is present in scope.
Limitations	The conclusion is limited to the sampled delegation; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.

Trust relationships

What is assessed	Damocles identifies trust direction, scope, authentication behaviour, filtering and reachable principals or resources across authorised domains or forests.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. Directory trust configuration, authorised identities in each relevant domain or forest, and filtering or selective-authentication settings.
Evidence	Trust direction and scope record with observed authentication and reachable principal or resource evidence.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Trust relationships when the directory relationship or authorised system is present in scope.
Limitations	Testing does not traverse excluded domains or alter trust configuration, and observed reachability does not establish all possible identities.

Local privilege paths

What is assessed	Damocles inspects local groups, endpoint rights, services, scheduled tasks, stored credentials and administrative access for a safe local privilege path.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. A supplied workstation or server foothold, standard identity, local policy and permission evidence.
Evidence	Host, identity, group, permission and configuration evidence supporting each local privilege step.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to authorised domain-joined endpoints where local privilege assessment is included.
Limitations	Validation stops after the minimum safe proof; excluded hosts, destructive service changes and persistence are not tested.

Domain privilege paths

What is assessed	Damocles analyses group nesting, ACLs, delegation, service accounts, certificate services, trusts and sessions and validates the least invasive domain privilege step.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. A standard domain identity, authorised directory queries, relevant ACL and certificate-service data, and named protected-account exclusions.
Evidence	A step-by-step identity and permission path with affected principals, ACLs, delegation and the safely validated transition.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Domain privilege paths when domain privilege escalation is authorised from the supplied starting identity.
Limitations	The result does not prove every directory path; password changes, persistence and impact to protected accounts are prohibited.

Administrative tiers

What is assessed	Damocles compares administrative identities, systems, group membership and permitted logon paths with the supplied tiering model.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. The intended tier model, administrative group membership, permitted logon matrix, representative admin identities and system inventory.
Evidence	Tier exception record identifying the principal, system, logon right or observed session that crosses the intended boundary.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Administrative tiers when the customer operates an administrative tiering or privileged-access model.
Limitations	A point-in-time sample cannot prove continuous adherence; Damocles does not use production privileged credentials beyond approved validation.

Management systems

What is assessed	Damocles identifies privileged management systems and tests whether representative identities can reach or authenticate to them contrary to intended administration paths.
Perspective / access	Directory privilege-path reviewer. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.

Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Authentication protocols

What is assessed	Damocles reviews and safely tests directory authentication protocols, signing, channel protection, delegation and fallback behaviour.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. A standard domain identity and workstation, domain policy, protocol configuration and approved authentication endpoints.
Evidence	Protocol negotiation, policy and delegation evidence tied to the tested identity and endpoint.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to the directory authentication protocols reachable from the authorised foothold.
Limitations	Credential relay, downgrade or coercion attempts stop at agreed safety thresholds and excluded accounts or systems are not targeted.

Identity attack-path chaining

What is assessed	Damocles connects credential, delegation, group, ACL, service-account and session observations into an ordered, reproducible identity privilege path.
Perspective / access	Standard domain user or workstation; Directory privilege-path reviewer. The supplied foothold, directory query access, authorised endpoints and the evidence gathered from preceding identity procedures.
Evidence	An ordered attack-path chain naming each principal, permission, credential, session or administrative relationship and the validated transition.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Identity attack-path chaining when multiple in-scope observations form a credible route to additional privilege or a sensitive identity.
Limitations	The chain is bounded to observed conditions and approved proof steps; it does not assert untested alternatives or authorise persistence.

Protected accounts and credential-testing limits

What is assessed	Damocles applies protected-account, authentication-attempt and credential-handling exclusions and records how they limit privilege-path coverage.
Perspective / access	Assumed internal foothold. Assessment requires a supplied foothold or domain identity, authorised directory queries, representative hosts and protected-account exclusions, selected specifically for protected accounts and credential-testing limits.
Evidence	Evidence records the principal, group, ACL, permission, host, session or ordered privilege-path evidence relevant to protected accounts and credential-testing limits.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Protected accounts and credential-testing limits when the directory relationship or authorised system is present in scope.

Limitations	The conclusion is limited to the sampled protected accounts and credential-testing limits; validation stops at minimum proof and excludes protected accounts, persistence and uncontrolled credential activity.
-------------	---

Methodologies and standards

Technical Guide to Information Security Testing and Assessment SP 800-115 — Uses NIST SP 800-115 guidance to plan, execute, analyse and report the authorised procedure.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Common Vulnerability Scoring System 4.0 — Calculates technical severity and records a CVSS 4.0 vector separately from customer impact.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised Active Directory and identity penetration testing scope.

Evidence: Coverage status, procedure results and findings can inform the customer’s control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Identity relationship map

Records identity relationship map produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Privilege-path chain

Records privilege-path chain produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Affected principal and permission evidence

Records affected principal and permission evidence produced from the authorised Active Directory and identity penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.