

# Descendant Credential Tetap Aktif Setelah Delegasi Dicabut

Format universal CyberSecAudit untuk lifecycle, offboarding, dan perubahan state setelah revoke.

| KATEGORI                | RISIKO                                                                                                                                                                                                                                                                                                                                                                                               | BUKTI            | CLEANUP  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|----------|
| Authorization Lifecycle | Medium · rekomendasi                                                                                                                                                                                                                                                                                                                                                                                 | Boundary crossed | Verified |
| 00                      | Pemberitahuan Publikasi<br>Rekonstruksi teredaksi dari pengujian terotorisasi. Nama target, domain, endpoint, akun, token, secret, identifier, dan bukti mentah tidak dipublikasikan.                                                                                                                                                                                                                |                  |          |
| 01                      | Ringkasan Eksekutif<br>Principal dengan delegasi sementara membuat descendant token. Setelah owner mencabut delegasi, credential sumber mati tetapi token turunan tetap dapat mengubah state.                                                                                                                                                                                                        |                  |          |
| 02                      | Security Invariant<br>Capability yang hanya ada karena delegasi sementara harus ikut dicabut ketika authorization source berakhir.                                                                                                                                                                                                                                                                   |                  |          |
| 03                      | Authority dan State Model<br>owner → delegated principal → descendant credential<br>ACTIVE → REVOKED                                                                                                                                                                                                                                                                                                 |                  |          |
| 04                      | Langkah Reproduksi <ul style="list-style-type: none"><li>• Aktifkan delegasi pada akun milik peneliti.</li><li>• Buat descendant credential melalui alur normal.</li><li>• Konfirmasi scope A diterima dan B ditolak.</li><li>• Owner mencabut delegasi.</li><li>• Konfirmasi source ditolak.</li><li>• Mutasi marker dengan descendant.</li><li>• Owner melakukan authoritative readback.</li></ul> |                  |          |
| 05                      | Proof Chain<br>delegation_active → PASS<br>descendant_create → SUCCESS<br>comparison_scope → DENIED<br>delegation_revoke → SUCCESS<br>source_after_revoke → DENIED<br>descendant_mutation → SUCCESS<br>authoritative_readback → MARKER MATCH                                                                                                                                                         |                  |          |

|    |                                                                                                                                                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 06 | Expected vs Actual<br>Expected: descendant ikut mati atau memerlukan izin persistence.<br>Actual: token tetap aktif sampai dihapus secara terpisah.                                                                  |
| 07 | Dampak Terverifikasi<br>Akses sementara berubah menjadi akses persisten dalam scope. Mutasi setelah revoke dibuktikan dari sesi owner.                                                                               |
| 08 | Negative Controls <ul style="list-style-type: none"> <li>• Source benar-benar ditolak setelah revoke.</li> <li>• Scope pembandingan tetap ditolak.</li> <li>• Marker dibaca melalui jalur owner terpisah.</li> </ul> |
| 09 | Batas Klaim<br>Tidak ada akses admin, cross-tenant, payment, resource berbayar, atau perubahan destruktif.                                                                                                           |
| 10 | Remediasi<br>Catat credential lineage, tambahkan permission persistence, cascade-revoke descendant, dan tampilkan inventory saat offboarding.                                                                        |
| 11 | Cleanup dan Retest<br>Marker dipulihkan, descendant dihapus dan menjadi ditolak, inventory kembali baseline.                                                                                                         |

## Konsultasi audit keamanan

<https://cybersecaudit.site/konsultasi> · [securityteam@cybersecaudit.site](mailto:securityteam@cybersecaudit.site)