INC0010101 — [TITAN] Critical — aml on stg-banking-aml-logs

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Closed
Resource	stg-banking-aml-logs	Group	banking_compliance
Resource type	Microsoft.Storage/storageAccounts	Change type	Emergency
Opened	2026-04-22 20:13:22	Closed	2026-04-22 20:27:22
CAB required	Yes	Close code	Successful

Security Finding

```
AML transaction log storage account publicly accessible — container 'aml-alerts' returns HTTP 200 anonymously. BSA/AML §1020.320 violation: customer identification and suspicious activity data must be protected.
```

Justification

```
Critical: AML transaction log storage account publicly accessible — container 'aml-alerts' returns HTTP 200 anonymously. BSA/AML §1020.320 violation: customer identification and suspicious activity data must be protected.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az storage account update --resource-group rg-banking-aml --name stgbankingamlogs --default-action Deny --allow-blob-public-access false
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: HIGH business risk — active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (stg-banking-aml-logs).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: AML transaction log storage account publicly accessible — container 'aml-alerts' returns HTTP 200 anonymously. BSA/AML §1020.320 violation: customer identification and suspicious activity data must be
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of stg-banking-aml-logs before change (baseline: titan-banking-demo-20260422T201922Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans stg-banking-aml-logs immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.
```

Recommended Fix Command

```
az storage account update --resource-group rg-banking-aml --name stgbankingamlogs --default-action Deny --allow-blob-public-access false
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, CIS 1.x IAM
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the critical aml incident, FORGE applied the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared, and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30 days for rollback.
```