INC0010007 — [TITAN] Low — security on alerts-prod-missing-rbac

Severity	Low	Priority	5 - Planning
Cloud	Azure	State	New
Resource	alerts-prod-missing-rbac	Group	identity_and_access
Resource type	Microsoft.Insights/alertRules	Change type	Incident
Opened	2026-04-21 15:26:55	Closed	2026-04-21 15:26:55
CAB required	No	Close code	—

Security Finding

```
No alert rule exists for 'Role Assignment Created at Subscription scope'. Detection gap for privilege escalation.
```

Justification

```
Low: No alert rule exists for 'Role Assignment Created at Subscription scope'. Detection gap for privilege escalation.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az monitor activity-log alert create --name rbac-subscription-scope --condition
category=Administrative AND operationName=Microsoft.Authorization/roleAssignments/write
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: LOW risk — hygiene item, fix during normal maintenance.
Business impact if unremediated: Minor deviation from baseline.
Scope: single resource (alerts-prod-missing-rbac).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: No alert rule exists for 'Role Assignment Created at Subscription scope'.
Detection gap for privilege escalation.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of alerts-prod-missing-rbac before change (baseline:
titan-killer-20260421T222654Z).
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 alerts-prod-missing-rbac 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 monitor activity-log alert create --name rbac-subscription-scope --condition
category=Administrative AND operationName=Microsoft.Authorization/roleAssignments/write
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1
```

AI Close Notes

```
2026-04-21 15:26:55 - System Administrator (Work notes)
[TITAN CONDUIT] Incident auto-filed from security scan.
Detecting agent: unknown (scan titan-killer-20260421T222654Z).
Severity: Low (priority 4).
This is a hygiene/access-control issue that does not require a CAB-gated change window. Assign to
the listed team and resolve per their standard runbook. TITAN will auto-detect clearance on the
next scan.
```