TITAN AI — GCP Live Scan

Report ID: **GCP-20260426-132448**

Customer: **TITAN AI Live Demo**

Generated: **2026-04-26T13:24:48.0631666-05:00**

Project: **adroit-terminus-234522**

Priority Buckets

Priority	Count	SLA
P1 (24 hours)	1	Internet-facing + PHI + exploit-in-wild stacked
P2 (72 hours)	8	Two-factor risk
P3 (next sprint)	0	Lower-risk / context-only

Severity Distribution

Severity	Count
Critical	1
High	8
Medium	0
Low	0

Findings — with priority, ATT&CK;, attack path, and remediation playbook

[P2] HIGH — IAM-SA on sa/1082937919292-compute@developer.gserviceaccount.com

Default Compute Engine service account is still active

Citation	CIS GCP 1.4, NIST 800-53 AC-6
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	PHI-exposure, Business-critical
MITRE ATT&CK	T1078.004 - Valid Accounts: Cloud Accounts
Attack path	SA Token Compromise > Project IAM > All Resources Authorized to Role
Path length	2 hops
Blast radius	1 service_account_or_binding
Recommendation	Disable the default compute SA; use dedicated SAs per workload.

Playbook — Security + IAM admin · 1-2 days

1. Identify what's still using the default Compute Engine SA: gcloud iam service-accounts get-iam-policy
2. Create a workload-specific SA with minimum-necessary roles
3. Migrate the workload to the new SA (Compute, GKE, Cloud Run, Cloud Functions all support SA swap)
4. Disable the default Compute SA: gcloud iam service-accounts disable

5. Add an Org Policy: iam.automaticIamGrantsForDefaultServiceAccounts -> false

[P2] HIGH — IAM on binding/roles/editor

Default Compute SA holds roles/editor on the project

Citation	CIS GCP 1.5, NIST 800-53 AC-6
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	PHI-exposure, Business-critical
MITRE ATT&CK	T1078.004 - Valid Accounts: Cloud Accounts
Attack path	SA Token Compromise > Project IAM > All Resources Authorized to Role
Path length	2 hops
Blast radius	1 service_account_or_binding
Recommendation	Replace with a least-privilege custom role bound to a workload-specific SA.

Playbook — Security + IAM admin · Same day

1. Identify all bindings granting Owner/Editor to default-compute SA: gcloud projects get-iam-policy
2. Replace with custom roles scoped to required APIs only (use Recommender to suggest minimum)
3. Update the workload's SA accordingly
4. Remove the broad role binding: gcloud projects remove-iam-policy-binding
5. Re-scan + verify workload still functions

[P2] HIGH — Firewall on fw/default-allow-rdp

Firewall rule default-allow-rdp exposes RDP (port 3389) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall default-allow-rdp > Compute Instance Network
Path length	2 hops
Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP
3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P2] HIGH — Firewall on fw/default-allow-ssh

Firewall rule default-allow-ssh exposes SSH (port 22) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3

Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall default-allow-ssh > Compute Instance Network
Path length	2 hops
Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP
3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P2] HIGH — Firewall on fw/fw-titandemo-bad-mssql-260426-1315

Firewall rule fw-titandemo-bad-mssql-260426-1315 exposes MSSQL (port 1433) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall fw-titandemo-bad-mssql-260426-1315 > Compute Instance Network
Path length	2 hops
Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP
3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P2] HIGH — Firewall on fw/fw-titandemo-bad-pg-260426-1315

Firewall rule fw-titandemo-bad-pg-260426-1315 exposes PostgreSQL (port 5432) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall fw-titandemo-bad-pg-260426-1315 > Compute Instance Network
Path length	2 hops

Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP
3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P2] HIGH — Firewall on fw/fw-titandemo-bad-rdp-260426-1315

Firewall rule fw-titandemo-bad-rdp-260426-1315 exposes RDP (port 3389) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall fw-titandemo-bad-rdp-260426-1315 > Compute Instance Network
Path length	2 hops
Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP
3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P2] HIGH — Firewall on fw/fw-titandemo-bad-ssh-260426-1315

Firewall rule fw-titandemo-bad-ssh-260426-1315 exposes SSH (port 22) to 0.0.0.0/0

Citation	CIS GCP 3.6/3.7, NIST 800-53 SC-7, PCI DSS 1.3
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > VPC Firewall fw-titandemo-bad-ssh-260426-1315 > Compute Instance Network
Path length	2 hops
Blast radius	1 firewall_rule
Recommendation	Restrict source range to corporate CIDR.

Playbook — Network + Security · 1-3 days

1. List all VMs reachable through this firewall rule's network
2. Update the rule's source range from 0.0.0.0/0 to corporate CIDR or use Identity-Aware Proxy for SSH/RDP

3. Enable VPC Flow Logs to detect any active traffic on this port from public internet
4. Add to Org Policy: enforce sourceRanges restriction on critical ports
5. Re-scan + audit flow logs for last 30 days

[P1] CRITICAL — GCS on gs://gs-titandemo-260426-1315-adroit-terminus-234522

Bucket gs-titandemo-260426-1315-adroit-terminus-234522 grants roles/storage.objectViewer to allUsers (PUBLIC)

Citation	HIPAA 164.312(a)(1), CIS GCP 5.1, NIST 800-53 AC-3
Priority	P1 • Fix in 24 hours • score 75/100
Risk factors	Internet-facing, PHI-exposure, Business-critical
MITRE ATT&CK	T1530 - Data from Cloud Storage
Attack path	Internet > GCS Public Endpoint > Bucket Objects
Path length	1 hops
Blast radius	1 gcs_bucket
Recommendation	Remove allUsers/allAuthenticatedUsers binding immediately.

Playbook — Storage Owner + Privacy · Same day

1. Remove allUsers/allAuthenticatedUsers binding: gcloud storage buckets remove-iam-policy-binding gs:// --member=allUsers --role=
2. Enable Uniform Bucket-Level Access: gcloud storage buckets update gs:// --uniform-bucket-level-access
3. Audit access logs for last 90 days for anonymous reads (Cloud Audit Logs)
4. If anonymous access to PHI/PII detected: trigger HIPAA breach assessment
5. Enable Sensitive Data Protection (DLP) inspection on the bucket