TITAN AI — AWS Live Scan

Report ID: **AWS-20260426-132246**

Customer: **TITAN AI Live Demo**

Generated: **2026-04-26T13:22:46.5817617-05:00**

Account: **450367038821** · Region: **us-east-1**

Priority Buckets

Priority	Count	SLA
P1 (24 hours)	2	Internet-facing + PHI + exploit-in-wild stacked
P2 (72 hours)	1	Two-factor risk
P3 (next sprint)	0	Lower-risk / context-only

Severity Distribution

Severity	Count
Critical	1
High	2
Medium	0
Low	0

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

[P1] CRITICAL — IAM on root-account/450367038821

Root user MFA is DISABLED

Citation	NIST 800-53 IA-2(1), CIS AWS 1.5, SOC2 CC6.1
Priority	P1 • Fix in 24 hours • score 75/100
Risk factors	PHI-exposure, Exploit-in-wild, Business-critical
MITRE ATT&CK	T1078.004 - Valid Accounts: Cloud Accounts
Attack path	Phish/Steal > Root Console > ALL AWS Resources
Path length	1 hops
Blast radius	1 entire_aws_account
Recommendation	Enable MFA on the root account immediately.

Playbook — Security + IAM admin · 30 minutes

1. Enable MFA on the root account via AWS console (only the root user can enable root MFA - cannot be delegated)
2. Delete any active root access keys: aws iam delete-access-key --user-name --access-key-id
3. For IAM users without MFA: aws iam enable-mfa-device --user-name --serial-number --authentication-code-1 --authentication-code-2
4. Add an SCP / IAM Boundary policy that denies actions when MFA is not present

5. Re-scan to verify root MFA enabled and no root keys

[P2] HIGH — IAM on user/iam-titandemo-260426-1311

IAM user iam-titandemo-260426-1311 has no MFA device

Citation	CIS AWS 1.10, NIST 800-53 IA-2
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	Phish/Steal > User Console > User-Authorized Resources
Path length	1 hops
Blast radius	1 iam_user
Recommendation	Require MFA on all human IAM users.

Playbook — Security + IAM admin · 30 minutes

1. Enable MFA on the root account via AWS console (only the root user can enable root MFA - cannot be delegated)
2. Delete any active root access keys: aws iam delete-access-key --user-name --access-key-id
3. For IAM users without MFA: aws iam enable-mfa-device --user-name --serial-number --authentication-code-1 --authentication-code-2
4. Add an SCP / IAM Boundary policy that denies actions when MFA is not present
5. Re-scan to verify root MFA enabled and no root keys

[P1] HIGH — S3 on s3://s3-titandemo-260426-1311-450367038821

S3 bucket s3-titandemo-260426-1311-450367038821 lacks full Public Access Block

Citation	HIPAA 164.312(a)(1), CIS AWS 2.1.5, 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 > S3 Public Endpoint > Bucket Objects
Path length	1 hops
Blast radius	1 s3_bucket
Recommendation	Enable all 4 Public Access Block settings (Block Public ACLs / Policy / Ignore / Restrict).

Playbook — Storage Owner + Privacy · Same day

1. Enable Public Access Block on the bucket: aws s3api put-public-access-block --bucket NAME --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
2. Enable default encryption: aws s3api put-bucket-encryption --bucket NAME --server-side-encryption-configuration with SSEAlgorithm AES256
3. Audit S3 access logs for last 90 days for anonymous reads
4. If anonymous access detected on PHI/PII bucket: trigger HIPAA breach assessment
5. Enable Macie for ongoing PII/PHI classification on the bucket