Cloud Security Assessment

Prepared by DeepDefence Technologies

AWS Account: 123456789012

Generated On: 3/9/2026, 12:32:56 pm

Executive Summary

SECURITY POSTURE: AT RISK

The assessment identified 2 high-impact failures. These gaps require attention to maintain infrastructure integrity.

Severity Summary

Risk Level	Failed	Total Checked
Critical	0	0
High	2	4
Medium	15	29
Low	3	3
Info	0	0

Detailed Vulnerability Findings (Failed Only)

Severity	Finding	Resource ID
High	Check S3 Account Level Public Access Block.	arn:aws:s3:us-east-1:123456789012:account
High	Ensure that general-purpose bucket policies restrict access to other AWS accounts.	arn:aws:s3:::grcy-list.venkatrv75
Medium	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to any port.	arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a
Medium	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to SSH port 22	arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a
Medium	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to Microsoft RDP port 3389	arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a
Medium	Security Groups created by EC2 Launch Wizard.	arn:aws:ec2:us-east-1:123456789012:security-group/sg-032633dd59b5a4f15
Medium	Check if IAM users have two active access keys	arn:aws:iam::123456789012:user/user2
Medium	Ensure users make use of temporary credentials assuming IAM roles	arn:aws:iam::123456789012:user/admin_user
Medium	Ensure users make use of temporary credentials assuming IAM roles	arn:aws:iam::123456789012:user/user2
Medium	Check if S3 buckets have event notifications enabled.	arn:aws:s3:::grcy-list.venkatrv75
Medium	Check if S3 buckets have event notifications enabled.	arn:aws:s3:::rv75-bck1
Medium	Check if S3 buckets have event notifications enabled.	arn:aws:s3:::rv75-bck3
Medium	Check if S3 buckets have KMS encryption enabled.	arn:aws:s3:::grcy-list.venkatrv75
Medium	Check if S3 buckets have KMS encryption enabled.	arn:aws:s3:::rv75-bck1

Severity	Finding	Resource ID
Medium	Check if S3 buckets have KMS encryption enabled.	arn:aws:s3:::stage-bck3
Medium	Check S3 Bucket Level Public Access Block.	arn:aws:s3:::grcy-list.stage
Medium	Check if S3 buckets have server access logging enabled	arn:aws:s3:::stage-bck3
Low	Check if S3 buckets use cross region replication.	arn:aws:s3:::grcy-list.stage
Low	Check if S3 buckets use cross region replication.	arn:aws:s3:::stage-bck1
Low	Check if S3 buckets use cross region replication.	arn:aws:s3:::stage-bck3

Technical Breakdown & Strategy

1. Check S3 Account Level Public Access Block.

Description: Check S3 Account Level Public Access Block.

Resource ID: arn:aws:s3:us-east-1:123456789012:account

Recommended Strategy:

Recommended Strategy: You can enable Public Access Block at the account level to prevent the exposure of your data stored in S3.

2. Ensure that general-purpose bucket policies restrict access to other AWS accounts.

Description: This check verifies that S3 bucket policies are configured in a way that limits access to the intended AWS accounts only, preventing unauthorized access by external or unintended accounts.

Resource ID: arn:aws:s3:::grcy-list.stage

Recommended Strategy:

Recommended Strategy: Review and update your S3 bucket policies to remove permissions that grant external AWS accounts access to critical actions and implement least privilege principles to ensure sensitive operations are restricted to trusted accounts only

3. Ensure no Network ACLs allow ingress from 0.0.0.0/0 to any port.

Description: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to any port.

Resource ID: arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a

Recommended Strategy:

Recommended Strategy: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive network acls. Recommended best practices is to narrow the definition for the minimum ports required.

4. Ensure no Network ACLs allow ingress from 0.0.0.0/0 to SSH port 22

Description: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to SSH port 22

Resource ID: arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a

Recommended Strategy:

Recommended Strategy: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive network acls. Recommended best practices is to narrow the definition for the minimum ports required.

5. Ensure no Network ACLs allow ingress from 0.0.0.0/0 to Microsoft RDP port 3389

Description: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to Microsoft RDP port 3389

Resource ID: arn:aws:ec2:us-east-1:123456789012:network-acl/acl-06b5acf115f2fcd5a

Recommended Strategy:

Recommended Strategy: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive network acls. Recommended best practices is to narrow the definition for the minimum ports required.

6. Security Groups created by EC2 Launch Wizard.

Description: Security Groups created by EC2 Launch Wizard.

Resource ID: arn:aws:ec2:us-east-1:123456789012:security-group/sg-032633dd59b5a4f15

Recommended Strategy:

Recommended Strategy: Apply Zero Trust approach. Implement a process to scan and remediate security groups created by the EC2 Wizard. Recommended best practices is to use an authorized security group.

7. Check if IAM users have two active access keys

Description: Check if IAM users have two active access keys

Resource ID: arn:aws:iam::123456789012:user/user2

Recommended Strategy:

Recommended Strategy: Avoid using long lived access keys.

8. Ensure users make use of temporary credentials assuming IAM roles

Description: Ensure users make use of temporary credentials assuming IAM roles

Resource ID: arn:aws:iam::123456789012:user/admin_user

Recommended Strategy:

Recommended Strategy: As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys.

9. Ensure users make use of temporary credentials assuming IAM roles

Description: Ensure users make use of temporary credentials assuming IAM roles

Resource ID: arn:aws:iam::123456789012:user/user2

Recommended Strategy:

Recommended Strategy: As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys.

10. Check if S3 buckets have event notifications enabled.

Description: Ensure whether S3 buckets have event notifications enabled.

Resource ID: arn:aws:s3:::grcy-list.stage

Recommended Strategy:

Recommended Strategy: Enable event notifications for all S3 general-purpose buckets to monitor important events such as object creation, deletion, tagging, and lifecycle events, ensuring visibility and quick action on relevant changes.

11. Check if S3 buckets have event notifications enabled.

Description: Ensure whether S3 buckets have event notifications enabled.

Resource ID: arn:aws:s3:::stage-bck1

Recommended Strategy:

Recommended Strategy: Enable event notifications for all S3 general-purpose buckets to monitor important events such as object creation, deletion, tagging, and lifecycle events, ensuring visibility and quick action on relevant changes.

12. Check if S3 buckets have event notifications enabled.

Description: Ensure whether S3 buckets have event notifications enabled.

Resource ID: arn:aws:s3:::stage-bck3

Recommended Strategy:

Recommended Strategy: Enable event notifications for all S3 general-purpose buckets to monitor important events such as object creation, deletion, tagging, and lifecycle events, ensuring visibility and quick action on relevant changes.

13. Check if S3 buckets have KMS encryption enabled.

Description: Check if S3 buckets have KMS encryption enabled.

Resource ID: arn:aws:s3:::grcy-list.stage

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have encryption at rest enabled using KMS.

14. Check if S3 buckets have KMS encryption enabled.

Description: Check if S3 buckets have KMS encryption enabled.

Resource ID: arn:aws:s3:::stage-bck1

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have encryption at rest enabled using KMS.

15. Check if S3 buckets have KMS encryption enabled.

Description: Check if S3 buckets have KMS encryption enabled.

Resource ID: arn:aws:s3:::stage-bck3

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have encryption at rest enabled using KMS.

16. Check S3 Bucket Level Public Access Block.

Description: Check S3 Bucket Level Public Access Block.

Resource ID: arn:aws:s3:::grcy-list.stage

Recommended Strategy:

Recommended Strategy: You can enable Public Access Block at the bucket level to prevent the exposure of your data stored in S3.

17. Check if S3 buckets have server access logging enabled

Description: Check if S3 buckets have server access logging enabled

Resource ID: arn:aws:s3:::stage-bck3

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have Logging enabled. CloudTrail data events can be used in place of S3 bucket logging. If that is the case, this finding can be considered a false positive.

18. Check if S3 buckets use cross region replication.

Description: Verifying whether S3 buckets have cross-region replication enabled, ensuring data redundancy and availability across multiple AWS regions

Resource ID: arn:aws:s3:::grcy-list.stage

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have cross region replication.

19. Check if S3 buckets use cross region replication.

Description: Verifying whether S3 buckets have cross-region replication enabled, ensuring data redundancy and availability across multiple AWS regions

Resource ID: arn:aws:s3:::stage-bck1

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have cross region replication.

20. Check if S3 buckets use cross region replication.

Description: Verifying whether S3 buckets have cross-region replication enabled, ensuring data redundancy and availability across multiple AWS regions

Resource ID: arn:aws:s3:::stage-bck3

Recommended Strategy:

Recommended Strategy: Ensure that S3 buckets have cross region replication.

Compliance Audit Log (Passed Checks)

Severity	Verified Control & Resource	Status
Medium	Security Groups created by EC2 Launch Wizard. Resource: arn:aws:ec2:ap-southeast-2:123456789012:security-group/sg-02e0fd38ab9018f99	PASS
Medium	Security Groups created by EC2 Launch Wizard. Resource: arn:aws:ec2:us-east-1:123456789012:security-group/sg-03d0e6ef5643207e7	PASS
Medium	Security Groups created by EC2 Launch Wizard. Resource: arn:aws:ec2:us-east-1:123456789012:security-group/sg-047d49825c3f5d631	PASS
Medium	Security Groups created by EC2 Launch Wizard. Resource: arn:aws:ec2:us-east-1:123456789012:security-group/sg-0d12a7407d1e48e31	PASS
Medium	Check if IAM users have two active access keys Resource: arn:aws:iam::123456789012:user/user1	PASS
Medium	Ensure users make use of temporary credentials assuming IAM roles Resource: arn:aws:iam::123456789012:user/security-user1	PASS
Medium	Ensure users make use of temporary credentials assuming IAM roles Resource: arn:aws:iam::123456789012:user/user1	PASS
Medium	Check if S3 buckets have ACLs enabled Resource: arn:aws:s3:::grcy-list.stage	PASS
Medium	Check if S3 buckets have ACLs enabled Resource: arn:aws:s3:::stage-bck1	PASS
Medium	Check if S3 buckets have ACLs enabled Resource: arn:aws:s3:::stage-bck3	PASS
High	Ensure that general-purpose bucket policies restrict access to other AWS accounts. Resource: arn:aws:s3:::stage-bck1	PASS
High	Ensure that general-purpose bucket policies restrict access to other AWS accounts. Resource: arn:aws:s3:::stage-bck3	PASS
Medium	Check if S3 buckets have default encryption (SSE) enabled or use a bucket policy to enforce it. Resource: arn:aws:s3:::grcy-list.stage	PASS
Medium	Check if S3 buckets have default encryption (SSE) enabled or use a bucket policy to enforce it. Resource: arn:aws:s3:::stage-bck1	PASS
Medium	Check if S3 buckets have default encryption (SSE) enabled or use a bucket policy to enforce it. Resource: arn:aws:s3:::stage-bck3	PASS
Medium	Check S3 Bucket Level Public Access Block. Resource: arn:aws:s3:::stage-bck1	PASS