Checkmarx

KICS REPORT vv1.5.2

HIGH	618	MEDIUM	320	LOW	116	INFO	424	TOTAL	1478

PLATFORMS Terraform, Common
START TIME 07:27:34, Mar 12 2022
END TIME 07:28:26, Mar 12 2022
SCANNED PATHS:
- test-cases/terraform/

AD Admin Not Configured For SQL Server

Results 2

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

The Active Directory Administrator is not configured for a SQL server

test-cases/terraform/azure/best-practices/sql_vulnerability_assessment_not_enabled/main.tf:15

Expected: A 'azurerm_sql_active_directory_administrator' is defined for 'azurerm_sql_server[sql]'

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:15

Expected: A 'azurerm_sql_active_directory_administrator' is defined for 'azurerm_sql_server[sql]'

ALB Listening on HTTP

Results 2

Severity HIGH
Platform Terraform
Category Networking and Firewall

Description

AWS Application Load Balancer (alb) should not listen on HTTP

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:70

Expected: 'default_action.redirect.protocol' is equal to 'HTTPS'

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:70

Expected: 'default_action.redirect.protocol' is equal to 'HTTPS'

AMI Not Encrypted

Results 1

Severity HIGH
Platform Terraform
Category Encryption

Description

AWS AMI Encryption is not enabled

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:38

Expected: One of 'rule.ebs_block_device.encrypted' is 'true'

App Service FTPS Enforce Disabled

Results 1

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Azure App Service should only enforce FTPS when 'ftps_state' is enabled

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:36

Checkmarx

KICS REPORT vv1.5.2

Expected: 'azurerm_app_service[webapp].site_config.ftps_state' is not set to 'AllAllowed'

App Service Managed Identity Disabled

Results 9

Severity	HIGH
Platform	Terraform
Category	Resource Management

Description

Azure App Service should have managed identity enabled

test-cases/terraform/azure/iam/webapp_not_use_managedidentity/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/encryption/in-transit/app_service_ftps_unused/main.tf:36

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/iam/app_service_authentication_missing/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/webapp_win_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/webapp_php_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/webapp_http2_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/iam/webapp_client_cert_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/webapp_lin_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].identity' is defined and not null

App Service Not Using Latest TLS Encryption Version

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Ensure App Service is using the latest version of TLS encryption

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:37

Expected: 'azurerm_app_service[webapp].site_config.min_tls_version' is set to '1.2'

Athena Database Not Encrypted

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

AWS Athena Database data in S3 should be encrypted

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:5

Expected: aws_athena_database[{{hoge}}] encryption_configuration is defined

Checkmarx

KICS REPORT vv1.5.2

Athena Workgroup Not Encrypted

Results 2

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Athena Workgroup query results should be encrypted, for all queries that run in the workgroup

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:25

Expected: aws_athena_workgroup[{{cloudrail_wg}}].configuration.result_configuration.encryption_configuration is defined

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:52

Expected: aws_athena_workgroup[{{cloudrail_wg_2}}].configuration.result_configuration.encryption_configuration is defined

Authentication Without MFA

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 1.10
Title	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password

Description

Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional credentials. With MFA enabled, when a user signs in to the AWS Console, they will be prompted for their user name and password as well as for an authentication code from their physical or virtual MFA token. It is recommended that MFA be enabled for all accounts that have a console password. Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that displays a time-sensitive key and have knowledge of a credential.

test-cases/terraform/aws/iam/iam-entities/iam_user_inline_policy_attach/main.tf:13

Expected: The attributes 'policy.Statement.Condition', 'policy.Statement.Condition.BoolIfExists', and 'policy.Statement.Condition.BoolIfExists.aws:MultiFactorAuthPresent' are defined and not null

Azure App Service Client Certificate Disabled

Results 9

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

Azure App Service client certificate should be enabled

test-cases/terraform/azure/iam/webapp_not_use_managedidentity/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/best-practices/webapp_php_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/best-practices/webapp_lin_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/best-practices/webapp_http2_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/encryption/in-transit/app_service_ftps_unused/main.tf:36

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:28

Checkmarx

KICS REPORT vv1.5.2

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/best-practices/webapp_win_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/iam/app_service_authentication_missing/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

test-cases/terraform/azure/iam/webapp_client_cert_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].client_cert_enabled' is defined

CMK Rotation Disabled

Results **3**

Severity	HIGH
Platform	Terraform
Category	Observability
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 3.8
Title	Ensure rotation for customer created CMKs is enabled

Description

AWS Key Management Service (KMS) allows customers to rotate the backing key which is key material stored within the KMS which is tied to the key ID of the Customer Created customer master key (CMK). It is the backing key that is used to perform cryptographic operations such as encryption and decryption. Automated key rotation currently retains all prior backing keys so that decryption of encrypted data can take place transparently. It is recommended that CMK key rotation be enabled. Rotating encryption keys helps reduce the potential impact of a compromised key as data encrypted with a new key cannot be accessed with a previous key that may have been exposed.

test-cases/terraform/aws/iam/iam-entities/policy_missing_principal/main.tf:5

Expected: aws_kms_key[secure_policy].enable_key_rotation is set to true

test-cases/terraform/aws/best-practices/kms_uses_rotation/main.tf:1

Expected: aws_kms_key[a].enable_key_rotation is set to true

test-cases/terraform/aws/iam/resource-policies/kms_key_not_secure_policy/main.tf:5

Expected: aws_kms_key[not_secure_policy].enable_key_rotation is set to true

CloudFront Without Minimum Protocol TLS 1.2

Results **4**

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

CloudFront Minimum Protocol version should be at least TLS 1.2

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:129

Expected: resource.aws_cloudfront_distribution[s3_distribution].viewer_certificate.cloudfront_default_certificate' is 'false'

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:109

Expected: resource.aws_cloudfront_distribution[s3_distribution].viewer_certificate.cloudfront_default_certificate' is 'false'

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:76

Expected: resource.aws_cloudfront_distribution[s3_distribution].viewer_certificate.cloudfront_default_certificate' is 'false'

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:115

Expected: resource.aws_cloudfront_distribution[s3_distribution].viewer_certificate.cloudfront_default_certificate' is 'false'

CloudTrail Log Files Not Encrypted

Results **3**

Checkmarx

KICS REPORT vv1.5.2

Severity	HIGH
Platform	Terraform
Category	Observability
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 3.7
Title	Ensure CloudTrail logs are encrypted at rest using KMS CMKs

Description

AWS CloudTrail is a web service that records AWS API calls for an account and makes those logs available to users and resources in accordance with IAM policies. AWS Key Management Service (KMS) is a managed service that helps create and control the encryption keys used to encrypt account data, and uses Hardware Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be configured to leverage server side encryption (SSE) and KMS customer created master keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be configured to use SSE-KMS. Configuring CloudTrail to use SSE-KMS provides additional confidentiality controls on log data as a given user must have S3 read permission on the corresponding log bucket and must be granted decrypt permission by the CMK policy.

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: aws_cloudtrail[foobar].kms_key_id is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: aws_cloudtrail[foobar].kms_key_id is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: aws_cloudtrail[foobar].kms_key_id is defined and not null

CloudTrail Log Files S3 Bucket with Logging Disabled

Results **3**

Severity	HIGH
Platform	Terraform
Category	Observability

Description

CloudTrail Log Files S3 Bucket should have 'logging' enabled

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: aws_s3_bucket[foo] has 'logging' defined

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: aws_s3_bucket[foo] has 'logging' defined

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: aws_s3_bucket[foo] has 'logging' defined

CloudWatch Log Group Not Encrypted

Results **2**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

AWS CloudWatch Log groups should be encrypted using KMS

test-cases/terraform/aws/encryption/at-rest/cloudwatch_groups_not_encrypted/main.tf:5

Expected: Attribute 'kms_key_id' is set

test-cases/terraform/aws/logging/cloudwatch_log_groups_no_retention/main.tf:5

Expected: Attribute 'kms_key_id' is set

Checkmarx

KICS REPORT vv1.5.2

CodeBuild Project Encrypted With AWS Managed Key

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

CodeBuild Project should be encrypted with customer-managed KMS keys instead of AWS managed keys

test-cases/terraform/aws/encryption/at-rest/codbuild_using_aws_key/main.tf:35

Expected: CodeBuild Project is not encrypted with AWS managed key

Configuration Aggregator to All Regions Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Observability
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 3.5
Title	Ensure AWS Config is enabled in all regions

Description

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended AWS Config be enabled in all regions. The AWS configuration item history captured by AWS Config enables security analysis, resource change tracking, and compliance auditing.

test-cases/terraform/aws/best-practices/config_aggregator_all_regions/main.tf:5

Expected: 'aws_config_configuration_aggregator[organization].account_aggregation_source.all_regions' is set to true

DAX Cluster Not Encrypted

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

AWS DAX Cluster should have server-side encryption at rest

test-cases/terraform/aws/encryption/at-rest/dax_cluster_not_encrypted/main.tf:25

Expected: aws_dax_cluster.server_side_encryption.enabled is set to true

DB Instance Publicly Accessible

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

The field 'publicly_accessible' should not be set to 'true' (default is 'false').

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:62

Expected: 'publicly_accessible' is set to false or undefined

DB Instance Storage Not Encrypted

Results 4

Severity	HIGH

Checkmarx

KICS REPORT vv1.5.2

Platform Terraform
Category Encryption

Description

The parameter storage_encrypted in aws_db_instance must be set to 'true' (the default is 'false').

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:113

Expected: 'storage_encrypted' is set to true

test-cases/terraform/aws/logging/rds_without_logging/main.tf:1

Expected: 'storage_encrypted' is set to true

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:60

Expected: 'storage_encrypted' is set to true

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:1

Expected: 'storage_encrypted' is set to true

DOCDB Cluster Not Encrypted

Results **2**

Severity HIGH
Platform Terraform
Category Encryption

Description

AWS DOCDB Cluster storage should be encrypted

test-cases/terraform/aws/encryption/at-rest/docdb_clusters_non_encrypted/main.tf:5

Expected: aws_docdb_cluster.storage_encrypted is set to true

test-cases/terraform/aws/logging/docdb_audit_logs_missing/main.tf:1

Expected: aws_docdb_cluster.storage_encrypted is set to true

DOCDB Cluster Without KMS

Results **3**

Severity HIGH
Platform Terraform
Category Encryption

Description

AWS DOCDB Cluster should be encrypted with a KMS encryption key

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_without_kms_key/main.tf:5

Expected: aws_docdb_cluster.kms_key_id is defined and not null

test-cases/terraform/aws/encryption/at-rest/docdb_clusters_non_encrypted/main.tf:5

Expected: aws_docdb_cluster.kms_key_id is defined and not null

test-cases/terraform/aws/logging/docdb_audit_logs_missing/main.tf:1

Expected: aws_docdb_cluster.kms_key_id is defined and not null

EBS Volume Snapshot Not Encrypted

Results **1**

Severity HIGH
Platform Terraform
Category Encryption

Description

The value on AWS EBS Volume Snapshot Encryptation must be true

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:24

Checkmarx

KICS REPORT vv1.5.2

Expected: 'aws_ebs_volume[example].encrypted' associated with aws_ebs_snapshot[example_snapshot] is set

EC2 Instance Has Public IP

Results **21**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

EC2 Instance should not have a public IP address.

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:83

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/ec2_ebs_not_optimized/main.tf:17

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:95

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/logging/ec2_without_monitoring/main.tf:17

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:93

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:63

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:87

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:45

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:61

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:80

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:31

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:108

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:141

Expected: 'associate_public_ip_address' is false

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:98

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:106

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:134

Expected: 'associate_public_ip_address' is false

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:136

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:149

Checkmarx

KICS REPORT vv1.5.2

Expected: 'associate_public_ip_address' is false

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:98

Expected: 'associate_public_ip_address' is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:82

Expected: 'associate_public_ip_address' is defined and not null

ECS Task Definition Volume Not Encrypted

Results **1**

Severity HIGH
Platform Terraform
Category Encryption

Description

AWS ECS Task Definition EFS data in transit between AWS ECS host and AWS EFS server should be encrypted

test-cases/terraform/aws/encryption/in-transit/ecs_task_definition_not_encrypted_in_transit/main.tf:44

Expected: aws_ecs_task_definition.volume.efs_volume_configuration.transit_encryption value is 'ENABLED'

EFS Not Encrypted

Results **2**

Severity HIGH
Platform Terraform
Category Encryption

Description

Elastic File System (EFS) must be encrypted

test-cases/terraform/aws/iam/resource-policies/efs_not_secure_policy/main.tf:5

Expected: aws_efs_file_system[not_secure].encrypted' is defined and not null

test-cases/terraform/aws/encryption/in-transit/ecs_task_definition_not_encrypted_in_transit/main.tf:5

Expected: aws_efs_file_system[test].encrypted' is defined and not null

EFS With Vulnerable Policy

Results **1**

Severity HIGH
Platform Terraform
Category Access Control

Description

EFS (Elastic File System) policy should avoid wildcard in 'Action' and 'Principal'.

test-cases/terraform/aws/iam/resource-policies/efs_not_secure_policy/main.tf:16

Expected: aws_efs_file_system_policy[not_secure_policy].policy does not have wildcard in 'Action' and 'Principal'

EFS Without KMS

Results **2**

Severity HIGH
Platform Terraform
Category Encryption

Description

Elastic File System (EFS) must have KMS Key ID

test-cases/terraform/aws/iam/resource-policies/efs_not_secure_policy/main.tf:5

Expected: aws_efs_file_system[not_secure].kms_key_id' is defined'

test-cases/terraform/aws/encryption/in-transit/ecs_task_definition_not_encrypted_in_transit/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_efs_file_system[test].kms_key_id' is defined'

EKS Cluster Encryption Disabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

EKS Cluster should be encrypted

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:19

Expected: 'encryption_config' is defined and not null

Function App Authentication Disabled

Results **9**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

Azure Function App authentication settings should be enabled

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:35

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:35

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:43

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:35

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:28

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

test-cases/terraform/azure/iam/func_app_authentication/main.tf:51

Expected: 'azurerm_function_app[functionapp].auth_settings.enabled' is set to true

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:46

Expected: 'azurerm_function_app[functionapp].auth_settings' is defined and not null

Function App FTPS Enforce Disabled

Results **6**

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Azure Function App should only enforce FTPS when 'ftps_state' is enabled

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:51

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:43

Checkmarx

KICS REPORT vv1.5.2

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:36

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is not set to 'AllAllowed'

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:51

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:43

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:60

Expected: 'azurerm_function_app[functionapp].site_config.ftps_state' is defined and not null

Function App Not Using Latest TLS Encryption Version

Results **1**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Ensure Function App is using the latest version of TLS encryption

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:44

Expected: 'azurerm_function_app[functionapp].site_config.min_tls_version' is set to '1.2'

Geo Redundancy Is Disabled

Results **4**

Severity	HIGH
Platform	Terraform
Category	Backup

Description

Make sure that on PostgreSQL Geo Redundant Backups is enabled

test-cases/terraform/azure/logging/postgresql_log_disconnections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server.example.geo_redundant_backup_enabled' is set

test-cases/terraform/azure/encryption/in-transit/postgresql_not_forcing_ssl/main.tf:15

Expected: 'azurerm_postgresql_server.example.geo_redundant_backup_enabled' is set

test-cases/terraform/azure/logging/postgresql_logcheckpoints_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server.example.geo_redundant_backup_enabled' is set

test-cases/terraform/azure/logging/postgresql_log_connections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server.example.geo_redundant_backup_enabled' is set

HTTP Port Open

Results **3**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

The HTTP port is open in a Security Group

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:129

Expected: aws_security_group.ingress doesn't open the HTTP port (80)

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:114

Expected: aws_security_group.ingress doesn't open the HTTP port (80)

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:121

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_security_group.ingress doesn't open the HTTP port (80)

IAM Database Auth Not Enabled

Results 4

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

IAM Database Auth Enabled must be configured to true

test-cases/terraform/aws/logging/rds_without_logging/main.tf:1

Expected: 'iam_database_authentication_enabled' is set to true

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:113

Expected: 'iam_database_authentication_enabled' is set to true

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:60

Expected: 'iam_database_authentication_enabled' is set to true

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:1

Expected: 'iam_database_authentication_enabled' is set to true

KMS Key With Vulnerable Policy

Results 2

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Checks if the policy is vulnerable and needs updating.

test-cases/terraform/aws/iam/resource-policies/kms_key_not_secure_policy/main.tf:9

Expected: aws_kms_key[not_secure_policy].policy does not have wildcard in 'Action' and 'Principal'

test-cases/terraform/aws/best-practices/kms_uses_rotation/main.tf:1

Expected: aws_kms_key[a].policy is defined and not null

Kinesis Not Encrypted With KMS

Results 2

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

AWS Kinesis Streams and metadata should be protected with KMS

test-cases/terraform/aws/encryption/at-rest/kinesis_stream_not_encrypted/main.tf:1

Expected: aws_kinesis_stream[test_stream].encryption_type is set

test-cases/terraform/aws/iam/resource-policies/cloudwatch_log_destination_insecure_policy/main.tf:49

Expected: aws_kinesis_stream[kinesis_for_cloudwatch].encryption_type is set

MSSQL Server Public Network Access Enabled

Results 5

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

MSSQL Server public network access should be disabled

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/azure/encryption/at-rest/sql_encryption_customer_key_not_set/main.tf:15

Expected: 'azurerm_mssql_server[sql].public_network_access_enabled' is defined and not null

test-cases/terraform/azure/iam/sql-server-ad-admin-not-set/main.tf:17

Expected: 'azurerm_mssql_server[sql].public_network_access_enabled' is defined and not null

test-cases/terraform/azure/logging/sql_server_audit_not_used/main.tf:17

Expected: 'azurerm_mssql_server[sql].public_network_access_enabled' is defined and not null

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:25

Expected: 'azurerm_mssql_server[sql].public_network_access_enabled' is defined and not null

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:28

Expected: 'azurerm_mssql_server[my-sql-server].public_network_access_enabled' is set to false

Memcached Disabled

Results **2**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Check if the Memcached is disabled on the ElastiCache

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:11

Expected: resource.aws_elasticache_cluster[disabled].engine enables Memcached

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:3

Expected: resource.aws_elasticache_cluster[default].engine enables Memcached

MySQL SSL Connection Disabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Make sure that for MySQL Database Server, 'Enforce SSL connection' is enabled

test-cases/terraform/azure/encryption/in-transit/mysql_not_forcing_ssl/main.tf:31

Expected: 'azurerm_mysql_server.example.ssl_enforcement_enabled' is equal 'true'

MySQL Server Public Access Enabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

MySQL Server public access should be disabled

test-cases/terraform/azure/encryption/in-transit/mysql_not_forcing_ssl/main.tf:33

Expected: 'azurerm_mysql_server[example].public_network_access_enabled' is set to false

Neptune Cluster Instance is Publicly Accessible

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

Neptune Cluster Instance should not be publicly accessible

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:82

Expected: aws_neptune_cluster_instance[neptune_instance].publicly_accessible is set to false

Passwords And Secrets - Generic Password

Results **33**

Severity	HIGH
Platform	Common
Category	Secret Management

Description

Query to find passwords and secrets in infrastructure code.

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:21

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/rds_cluster_encrypt_at_rest_disabled/main.tf:12

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:8

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/best-practices/vm_unmanaged_disks/main.tf:81

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/logging/docdb_audit_logs_missing/main.tf:5

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:83

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:27

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:8

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/sql_server_audit_not_used/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/vmss_win_diagnostic_log_disabled/main.tf:55

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_at_rest_using_cmk_not_customer_managed/main.tf:13

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/encryption/in-transit/postgresql_not_forcing_ssl/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:9

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:106

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:31

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/docdb_clusters_non_encrypted/main.tf:9

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:34

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/logging/rds_without_logging/main.tf:8

Checkmarx

KICS REPORT vv1.5.2

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/postgresql_logcheckpoints_not_enabled/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/postgresql_log_disconnections_not_enabled/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_without_kms_key/main.tf:9

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/encryption/at-rest/sql_encryption_customer_key_not_set/main.tf:21

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:5

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/networking/vm_public_rdp_lb_opened/main.tf:117

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/encryption/in-transit/mysql_not_forcing_ssl/main.tf:21

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/logging/postgresql_log_connections_not_enabled/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:124

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/networking/vmss_public_rdp_lb_opened/main.tf:79

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:120

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:34

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/networking/vm_public_rdp_nat_opened/main.tf:110

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/iam/sql-server-ad-admin-not-set/main.tf:23

Expected: Hardcoded secret key should not appear in source

test-cases/terraform/azure/best-practices/sql_vulnerability_assessment_not_enabled/main.tf:21

Expected: Hardcoded secret key should not appear in source

PostgreSQL Server Threat Detection Policy Disabled

Results **4**

Severity HIGH
Platform Terraform
Category Resource Management

Description

PostgreSQL Server Threat Detection Policy should be enabled

test-cases/terraform/azure/logging/postgresql_log_connections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server[example].threat_detection_policy' is a defined object

test-cases/terraform/azure/logging/postgresql_log_disconnections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server[example].threat_detection_policy' is a defined object

test-cases/terraform/azure/encryption/in-transit/postgresql_not_forcing_ssl/main.tf:15

Expected: 'azurerm_postgresql_server[example].threat_detection_policy' is a defined object

test-cases/terraform/azure/logging/postgresql_logcheckpoints_not_enabled/main.tf:15

Checkmarx

KICS REPORT vv1.5.2

Expected: 'azurerm_postgresql_server[example].threat_detection_policy' is a defined object

RDS Storage Not Encrypted

Results 2

Severity	HIGH
Platform	Terraform
Category	Encryption
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.3.1
Title	Ensure that encryption is enabled for RDS Instances

Description

Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances. After your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. Databases are likely to hold sensitive and critical data, it is highly recommended to implement encryption in order to protect your data from unauthorized access or disclosure. With RDS encryption enabled, the data stored on the instance's underlying storage, the automated backups, read replicas, and snapshots, are all encrypted.

test-cases/terraform/aws/encryption/at-rest/rds_cluster_encrypt_at_rest_disabled/main.tf:5

Expected: aws_rds_cluster.storage_encrypted is set to true

test-cases/terraform/aws/best-practices/rds_retention_period_set/main.tf:1

Expected: aws_rds_cluster.storage_encrypted is set to true

Redshift Not Encrypted

Results 4

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Check if 'encrypted' field is false or undefined (default is false)

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:103

Expected: aws_redshift_cluster.encrypted is defined and not null

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Expected: aws_redshift_cluster.encrypted is defined and not null

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster.encrypted is defined and not null

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster.encrypted is defined and not null

Redshift Publicly Accessible

Results 3

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Check if 'publicly_accessible' field is true or undefined (default is true)

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster.publicly_accessible is defined and not null

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_redshift_cluster.publicly_accessible is defined and not null

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster.publicly_accessible is defined and not null

Remote Desktop Port Open

Results **3**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

The Remote Desktop port is open in a Security Group

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:114

Expected: aws_security_group[publicly_accessible_sg].ingress doesn't open the remote desktop port (3389)

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:121

Expected: aws_security_group[publicly_accessible_sg].ingress doesn't open the remote desktop port (3389)

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:129

Expected: aws_security_group[publicly_accessible_sg].ingress doesn't open the remote desktop port (3389)

S3 Bucket ACL Allows Read Or Write to All Users

Results **3**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

S3 bucket with public READ/WRITE access

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:7

Expected: 'acl' is equal 'private'

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:16

Expected: 'acl' is equal 'private'

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:7

Expected: 'acl' is equal 'private'

S3 Bucket ACL Allows Read to Any Authenticated User

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

Misconfigured S3 buckets can leak private information to the entire internet or allow unauthorized data tampering / deletion

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:7

Expected: aws_s3_bucket[public-bucket].acl is private

S3 Bucket Access to Any Principal

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

Checkmarx

KICS REPORT vv1.5.2

S3 Buckets must not allow Actions From All Principals, as to prevent leaking private information to the entire internet or allow unauthorized data tampering / deletion. This means the 'Effect' must not be 'Allow' when there are All Principals

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:12

Expected: aws_s3_bucket_policy[bucket_2_policy].policy.Principal is not equal to, nor does it contain '*'

S3 Bucket Allows Get Action From All Principals

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

S3 Buckets must not allow Get Action From All Principals, as to prevent leaking private information to the entire internet or allow unauthorized data tampering / deletion. This means the 'Effect' must not be 'Allow' when the 'Action' is Get, for all Principals.

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:20

Expected: aws_s3_bucket_policy[bucket_2_policy].policy.Action is not a 'Get' action

S3 Bucket Object Not Encrypted

Results **1**

Severity	HIGH
Platform	Terraform
Category	Encryption
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.1.1
Title	Ensure all S3 buckets employ encryption-at-rest

Description

Amazon S3 provides a variety of no, or low, cost encryption options to protect data at rest. Encrypting data at rest reduces the likelihood that it is unintentionally exposed and can nullify the impact of disclosure if the encryption remains unbroken.

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:18

Expected: aws_s3_bucket_object.server_side_encryption is defined and not null

S3 Bucket SSE Disabled

Results **19**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

If algorithm is AES256 then the master key is null, empty or undefined, otherwise the master key is required

test-cases/terraform/aws/logging/s3_access_logging_disabled/main.tf:1

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:1

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:32

Expected: 'server_side_encryption_configuration' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:14

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:1

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_non_encrypted/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:33

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:1

Expected: 'server_side_encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

S3 Bucket Without Enabled MFA Delete

Results **19**

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.1.3
Title	Ensure MFA Delete is enable on S3 buckets

Description

Once MFA Delete is enabled on your sensitive and classified S3 bucket it requires the user to have two forms of authentication. Adding MFA delete to an S3 bucket, requires additional authentication when you change the version state of your bucket or you delete and object version adding another layer of security in the event your security credentials are compromised or unauthorized access is granted.

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Expected: aws_s3_bucket[public-bucket].versioning is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: aws_s3_bucket[public-bucket].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:32

Expected: aws_s3_bucket[cloudrail_anthena_bucket_2].versioning is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:5

Expected: aws_s3_bucket[logging].versioning is defined and not null

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:1

Expected: aws_s3_bucket[b].versioning is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: aws_s3_bucket[public-bucket].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:1

Expected: aws_s3_bucket[hoge].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:5

Expected: aws_s3_bucket[cloudrail].versioning is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: aws_s3_bucket[foo].versioning is defined and not null

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:1

Expected: aws_s3_bucket[b].versioning is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: aws_s3_bucket[foo].versioning is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:14

Expected: aws_s3_bucket[dist].versioning is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:33

Expected: aws_s3_bucket[cloudrail].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_non_encrypted/main.tf:5

Expected: aws_s3_bucket[cloudrail].versioning is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: aws_s3_bucket[cdn-content].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:5

Expected: aws_s3_bucket[cloudrail_anthena_bucket].versioning is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: aws_s3_bucket[public-bucket].versioning is defined and not null

test-cases/terraform/aws/logging/s3_access_logging_disabled/main.tf:1

Expected: aws_s3_bucket[b].versioning is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: aws_s3_bucket[foo].versioning is defined and not null

SQL Database Audit Disabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Resource Management

Description

Ensure that 'Threat Detection' is enabled for Azure SQL Database

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:43

Expected: 'threat_detection_policy' exists

Checkmarx

KICS REPORT vv1.5.2

SQS With SSE Disabled

Results 4

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Amazon Simple Queue Service (SQS) queue is not protecting the contents of their messages using Server-Side Encryption (SSE)

test-cases/terraform/aws/best-practices/tag_all_items/plan.json:1

Expected: aws_sqs_queue.kms_master_key_id is defined and not null

test-cases/terraform/aws/encryption/at-rest/sqs_queue_not_encrypted/main.tf:5

Expected: aws_sqs_queue.kms_master_key_id is defined and not null

test-cases/terraform/aws/best-practices/tag_all_items/main.tf:12

Expected: aws_sqs_queue.kms_master_key_id is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:103

Expected: aws_sqs_queue.kms_master_key_id is defined and not null

SSL Enforce Disabled

Results 1

Severity HIGH
Platform Terraform
Category Encryption

Description

Make sure that for PosgreSQL, the 'Enforce SSL connection' is set to 'ENABLED'

test-cases/terraform/azure/encryption/in-transit/postgresql_not_forcing_ssl/main.tf:25

Expected: 'azurerm_postgresql_server.example.ssl_enforcement_enabled' is equal 'true'

Sagemaker Notebook Instance Without KMS

Results 1

Severity HIGH
Platform Terraform
Category Encryption

Description

AWS SageMaker should encrypt model artifacts at rest using Amazon S3 server-side encryption with an AWS KMS

test-cases/terraform/aws/encryption/at-rest/sagemaker_not_encrypted/main.tf:23

Expected: aws_sagemaker_notebook_instance.kms_key_id is defined and not null

Security Group With Unrestricted Access To SSH

Results 3

Severity HIGH
Platform Terraform
Category Networking and Firewall

Description

'SSH' (TCP:22) should not be public in AWS Security Group

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:135

Expected: aws_security_group[publicly_accessible_sg] 'SSH' (Port:22) is not public

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:127

Expected: aws_security_group[publicly_accessible_sg] 'SSH' (Port:22) is not public

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:120

Expected: aws_security_group[publicly_accessible_sg] 'SSH' (Port:22) is not public

Sensitive Port Is Exposed To Entire Network

Results **311**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

A sensitive port, such as port 23 or port 110, is open for the whole network in either TCP or UDP protocol

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: HTTP (TCP:80) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: HDFS NameNode WebUI (TCP:50470) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra Monitoring (TCP:7199) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: POP3 (TCP:110) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: VNC Server (TCP:5900) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SQL Server Analysis (TCP:2382) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Known internal web port (TCP:8000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra Thrift (TCP:9160) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: POP3 (TCP:110) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Memcached SSL (TCP:11214) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: LDAP SSL (TCP:636) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra OpsCenter (TCP:61621) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra OpsCenter Website (TCP:8888) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: FTP (TCP:21) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Memcached SSL (TCP:11214) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: VNC Listener (TCP:5500) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Puppet Master (TCP:8140) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Checkmarx

KICS REPORT vv1.5.2

Expected: DNS (TCP:53) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra (TCP:7001) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SMTP (TCP:25) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Memcached SSL (TCP:11215) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: LDAP (TCP:389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: HTTP (TCP:80) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Oracle DB SSL (TCP:2483) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: POP3 (TCP:110) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Microsoft-DS (TCP:445) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Memcached SSL (TCP:11214) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SaltStack Master (TCP:4505) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Hadoop Name Node (TCP:9000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: MSSQL Server (TCP:1433) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: HDFS NameNode (TCP:8020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SQL Server Analysis (TCP:2383) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: MSSQL Browser (TCP:1434) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: PostgreSQL (TCP:5432) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: LDAP SSL (TCP:636) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SMTP (TCP:25) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: HDFS NameNode WebUI (TCP:50470) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Oracle Auto Data Warehouse (TCP:1522) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Docker (TCP:2376) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Memcached SSL (TCP:11215) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra OpsCenter (TCP:61621) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra OpsCenter (TCP:61620) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SMTP (TCP:25) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: HTTP (TCP:80) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Oracle DB SSL (TCP:2483) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: PostgreSQL (TCP:5432) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: VNC Listener (TCP:5500) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Mongo Web Portal (TCP:27018) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra OpsCenter Website (TCP:8888) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Prevalent known internal port (TCP:3000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: VNC Listener (TCP:5500) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: CIFS / SMB (TCP:3020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Telnet (TCP:23) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Docker (TCP:2375) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Mongo (TCP:27017) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Hadoop Name Node (TCP:9000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Hadoop Name Node (TCP:9000) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra OpsCenter (TCP:61621) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: MSSQL Server (TCP:1433) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: FTP (TCP:20) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Kibana (TCP:5601) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Checkmarx

KICS REPORT vv1.5.2

Expected: Oracle DB SSL (TCP:2484) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra Internode Communication (TCP:7000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: MySQL (TCP:3306) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra (TCP:7001) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: LDAP SSL (TCP:636) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Elastic Search (TCP:9200) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Elastic Search (TCP:9200) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Known internal web port (TCP:8000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Oracl DB (TCP:1521) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Puppet Master (TCP:8140) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra Monitoring (TCP:7199) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra Thrift (TCP:9160) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SQL Server Analysis (TCP:2382) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Docker (TCP:2376) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Elastic Search (TCP:9300) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Mongo (TCP:27017) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SaltStack Master (TCP:4506) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: FTP (TCP:20) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SaltStack Master (TCP:4506) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra OpsCenter Website (TCP:8888) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Oracle Auto Data Warehouse (TCP:1522) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: WinRM for HTTP (TCP:5985) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: NetBIOS Session Service (TCP:139) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: MSSQL Debugger (TCP:135) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Redis (TCP:6379) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra OpsCenter Website (TCP:8888) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SSH (TCP:22) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: HDFS NameNode WebUI (TCP:50470) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SSH (TCP:22) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Mongo Web Portal (TCP:27018) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: NetBIOS Name Service (TCP:137) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: NetBIOS Session Service (TCP:139) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Memcached (TCP:11211) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: MSSQL Debugger (TCP:135) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Elastic Search (TCP:9300) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Memcached SSL (TCP:11215) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Known internal web port (TCP:8080) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Oracl DB (TCP:1521) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: CiscoSecure, WebSM (TCP:9090) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Memcached (TCP:11211) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Oracl DB (TCP:1521) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra OpsCenter (TCP:61620) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Kibana (TCP:5601) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: NetBIOS Name Service (TCP:137) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Prevalent known internal port (TCP:3000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Checkmarx

KICS REPORT vv1.5.2

Expected: Cassandra Internode Communication (TCP:7000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Elastic Search (TCP:9200) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: NetBIOS Name Service (TCP:137) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: NetBIOS Datagram Service (TCP:138) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Docker (TCP:2375) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: MySQL (TCP:3306) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SMTP (TCP:25) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Memcached SSL (TCP:11215) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Puppet Master (TCP:8140) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SaltStack Master (TCP:4506) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SNMP (TCP:161) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Remote Desktop (TCP:3389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra (TCP:7001) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Mongo (TCP:27017) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: DNS (TCP:53) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: VNC Listener (TCP:5500) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SaltStack Master (TCP:4506) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: VNC Server (TCP:5900) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Kibana (TCP:5601) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: NetBIOS Name Service (TCP:137) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Elastic Search (TCP:9200) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Known internal web port (TCP:8000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Oracle DB SSL (TCP:2483) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SQL Server Analysis (TCP:2383) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SaltStack Master (TCP:4506) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: WinRM for HTTP (TCP:5985) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: NetBIOS Name Service (TCP:137) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SaltStack Master (TCP:4505) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: NetBIOS Datagram Service (TCP:138) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: POP3 (TCP:110) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SQL Server Analysis (TCP:2383) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Remote Desktop (TCP:3389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: CIFS / SMB (TCP:3020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: SNMP (TCP:161) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Puppet Master (TCP:8140) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: HDFS NameNode (TCP:8020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: HDFS NameNode (TCP:8020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: PostgreSQL (TCP:5432) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra OpsCenter Website (TCP:8888) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: FTP (TCP:20) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Mongo Web Portal (TCP:27018) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: MSSQL Browser (TCP:1434) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: HDFS NameNode WebUI (TCP:50070) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: HTTP (TCP:80) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Microsoft-DS (TCP:445) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Checkmarx

KICS REPORT vv1.5.2

Expected: Memcached (TCP:11211) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Memcached SSL (TCP:11215) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Redis (TCP:6379) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra Client (TCP:9042) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Mongo (TCP:27017) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Remote Desktop (TCP:3389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra OpsCenter (TCP:61620) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Docker (TCP:2375) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Telnet (TCP:23) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: VNC Server (TCP:5900) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra OpsCenter (TCP:61621) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: HDFS NameNode (TCP:8020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: NetBIOS Datagram Service (TCP:138) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Elastic Search (TCP:9300) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: POP3 (TCP:110) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SSH (TCP:22) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: SaltStack Master (TCP:4505) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: MSSQL Debugger (TCP:135) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra OpsCenter (TCP:61620) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SSH (TCP:22) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra OpsCenter (TCP:61620) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: MSSQL Debugger (TCP:135) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Redis (TCP:6379) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: LDAP (TCP:389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Microsoft-DS (TCP:445) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra Monitoring (TCP:7199) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Oracle Auto Data Warehouse (TCP:1522) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Known internal web port (TCP:8080) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra Monitoring (TCP:7199) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SMTP (TCP:25) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SSH (TCP:22) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SQL Server Analysis (TCP:2383) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: MSSQL Browser (TCP:1434) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: VNC Server (TCP:5900) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Redis (TCP:6379) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra Internode Communication (TCP:7000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra Thrift (TCP:9160) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra (TCP:7001) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Elastic Search (TCP:9300) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Prevalent known internal port (TCP:3000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Telnet (TCP:23) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Mongo (TCP:27017) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra (TCP:7001) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Expected: FTP (TCP:20) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: MSSQL Server (TCP:1433) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: HDFS NameNode WebUI (TCP:50470) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Remote Desktop (TCP:3389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: MSSQL Server (TCP:1433) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SQL Server Analysis (TCP:2382) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: VNC Server (TCP:5900) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: DNS (TCP:53) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Memcached (TCP:11211) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra Thrift (TCP:9160) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: PostgreSQL (TCP:5432) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SNMP (TCP:161) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Known internal web port (TCP:8080) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: CiscoSecure, WebSM (TCP:9090) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: DNS (TCP:53) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: LDAP (TCP:389) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Oracle DB SSL (TCP:2483) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: HDFS NameNode WebUI (TCP:50070) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Docker (TCP:2376) should not be allowed

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:12

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Mongo Web Portal (TCP:27018) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: MSSQL Browser (TCP:1434) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: HDFS NameNode (TCP:8020) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: HDFS NameNode WebUI (TCP:50070) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Oracl DB (TCP:1521) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Oracle DB SSL (TCP:2484) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: LDAP SSL (TCP:636) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: CiscoSecure, WebSM (TCP:9090) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Oracle Auto Data Warehouse (TCP:1522) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Docker (TCP:2376) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Oracle DB SSL (TCP:2483) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SQL Server Analysis (TCP:2383) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Docker (TCP:2376) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Oracle DB SSL (TCP:2484) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: FTP (TCP:21) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: LDAP SSL (TCP:636) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Cassandra Client (TCP:9042) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: NetBIOS Datagram Service (TCP:138) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Docker (TCP:2375) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SQL Server Analysis (TCP:2382) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Docker (TCP:2375) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: HDFS NameNode WebUI (TCP:50070) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Prevalent known internal port (TCP:3000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Checkmarx

KICS REPORT vv1.5.2

Expected: Cassandra Client (TCP:9042) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SQL Server Analysis (TCP:2382) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Elastic Search (TCP:9200) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Known internal web port (TCP:8000) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: VNC Listener (TCP:5500) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Known internal web port (TCP:8080) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: WinRM for HTTP (TCP:5985) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Microsoft-DS (TCP:445) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Memcached SSL (TCP:11214) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra Thrift (TCP:9160) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Elastic Search (TCP:9300) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Hadoop Name Node (TCP:9000) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Telnet (TCP:23) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Kibana (TCP:5601) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Microsoft-DS (TCP:445) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: MSSQL Browser (TCP:1434) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Hadoop Name Node (TCP:9000) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: CIFS / SMB (TCP:3020) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: MySQL (TCP:3306) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: HDFS NameNode WebUI (TCP:50070) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Telnet (TCP:23) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SaltStack Master (TCP:4505) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: CIFS / SMB (TCP:3020) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: CIFS / SMB (TCP:3020) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: NetBIOS Datagram Service (TCP:138) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Known internal web port (TCP:8080) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: MSSQL Server (TCP:1433) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: HDFS NameNode WebUI (TCP:50470) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: PostgreSQL (TCP:5432) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Puppet Master (TCP:8140) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Memcached SSL (TCP:11214) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra Client (TCP:9042) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: FTP (TCP:21) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: NetBIOS Session Service (TCP:139) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: SNMP (TCP:161) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: WinRM for HTTP (TCP:5985) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: MySQL (TCP:3306) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: MySQL (TCP:3306) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Kibana (TCP:5601) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Cassandra Client (TCP:9042) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: NetBIOS Session Service (TCP:139) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: CiscoSecure, WebSM (TCP:9090) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Cassandra Internode Communication (TCP:7000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Cassandra Monitoring (TCP:7199) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Mongo Web Portal (TCP:27018) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Checkmarx

KICS REPORT vv1.5.2

Expected: WinRM for HTTP (TCP:5985) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: HTTP (TCP:80) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: SaltStack Master (TCP:4505) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Redis (TCP:6379) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: MSSQL Debugger (TCP:135) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra OpsCenter (TCP:61621) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: NetBIOS Session Service (TCP:139) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: CiscoSecure, WebSM (TCP:9090) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Prevalent known internal port (TCP:3000) should not be allowed

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: Remote Desktop (TCP:3389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: Oracl DB (TCP:1521) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Oracle DB SSL (TCP:2484) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: LDAP (TCP:389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: FTP (TCP:21) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: DNS (TCP:53) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Oracle Auto Data Warehouse (TCP:1522) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: FTP (TCP:20) should not be allowed

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: Oracle DB SSL (TCP:2484) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: LDAP (TCP:389) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: Cassandra Internode Communication (TCP:7000) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Memcached (TCP:11211) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: FTP (TCP:21) should not be allowed

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: Known internal web port (TCP:8000) should not be allowed

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: SNMP (TCP:161) should not be allowed

Storage Account Not Forcing HTTPS

Results **20**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

See that Storage Accounts forces the use of HTTPS

test-cases/terraform/azure/iam/func_app_authentication/main.tf:22

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/encryption/at-rest/storacc_encryption_not_enabled/main.tf:18

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:24

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:17

Expected: 'azurerm_storage_account.example.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:23

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/logging/iot_hub_diagnostic_not_enabled/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:35

Expected: 'azurerm_storage_account.my-storage-account.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:11

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:24

Expected: 'azurerm_storage_account.example.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/vm_unmanaged_disks/main.tf:42

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/encryption/at-rest/activitylog_storage_account_encryption_not_enabled/main.tf:18

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:41

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/logging/batch_diagnostic_disabled/main.tf:15

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/azure/logging/vmss_win_diagnostic_log_disabled/main.tf:41

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

test-cases/terraform/azure/iam/storage_account_public_access_disabled/main.tf:16

Expected: 'azurerm_storage_account.storacc.enable_https_traffic_only' equals 'true'

Trusted Microsoft Services Not Enabled

Results **20**

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Trusted MIcrosoft Services are not enabled for Storage Account access

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:24

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:24

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/vm_unmanaged_disks/main.tf:42

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/iam/storage_account_public_access_disabled/main.tf:16

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/logging/iot_hub_diagnostic_not_enabled/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:41

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:35

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:11

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/logging/batch_diagnostic_disabled/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:17

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:15

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/encryption/at-rest/activitylog_storage_account_encryption_not_enabled/main.tf:18

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:23

Expected: 'network_rules' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/azure/logging/vmss_win_diagnostic_log_disabled/main.tf:41

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/iam/func_app_authentication/main.tf:22

Expected: 'network_rules' is defined and not null

test-cases/terraform/azure/encryption/at-rest/storacc_encryption_not_enabled/main.tf:18

Expected: 'network_rules' is defined and not null

Unknown Port Exposed To Internet

Results **6**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

AWS Security Group should not have an unknown port exposed to the entire Internet

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:25

Expected: aws_security_group[free].ingress.from_port is known

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:135

Expected: aws_security_group[publicly_accessible_sg].ingress.from_port is known

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:17

Expected: aws_security_group[allow_tls].ingress.from_port is known

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:16

Expected: aws_security_group[nondefault].ingress.from_port is known

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:120

Expected: aws_security_group[publicly_accessible_sg].ingress.from_port is known

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:127

Expected: aws_security_group[publicly_accessible_sg].ingress.from_port is known

Unrestricted Security Group Ingress

Results **6**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

Security groups allow ingress from 0.0.0.0:0

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:16

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:127

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:25

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:17

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:135

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:120

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

Checkmarx

KICS REPORT vv1.5.2

VPC Peering Route Table with Unrestricted CIDR

Results 1

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

VPC Peering Route Table should restrict CIDR

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:164

Expected: aws_route[subnet2_1].route restricts CIDR

Viewer Protocol Policy Allows HTTP

Results 6

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Checks if the connection between the CloudFront and the origin server is encrypted

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:50

Expected: resource.aws_cloudfront_distribution[s3_distribution].default_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:118

Expected: resource.aws_cloudfront_distribution[s3_distribution].ordered_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:44

Expected: resource.aws_cloudfront_distribution[s3_distribution].default_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:83

Expected: resource.aws_cloudfront_distribution[s3_distribution].default_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:100

Expected: resource.aws_cloudfront_distribution[s3_distribution].ordered_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:64

Expected: resource.aws_cloudfront_distribution[s3_distribution].default_cache_behavior.viewer_protocol_policy is 'https-only' or 'redirect-to-https'

Vulnerable Default SSL Certificate

Results 4

Severity	HIGH
Platform	Terraform
Category	Insecure Defaults

Description

CloudFront web distributions should use custom (and not default) SSL certificates. Custom SSL certificates allow only defined users to access content by using an alternate domain name instead of the default one.

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:114

Expected: Attribute 'cloudfront_default_certificate' is 'false' or not defined

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:128

Expected: Attribute 'cloudfront_default_certificate' is 'false' or not defined

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:108

Expected: Attribute 'cloudfront_default_certificate' is 'false' or not defined

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:75

Expected: Attribute 'cloudfront_default_certificate' is 'false' or not defined

Checkmarx

KICS REPORT vv1.5.2

Web App Accepting Traffic Other Than HTTPS

Results 9

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Web app should only accept HTTPS traffic in Azure Web App Service.

test-cases/terraform/azure/best-practices/webapp_win_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/iam/app_service_authentication_missing/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/best-practices/webapp_http2_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/iam/webapp_not_use_managedidentity/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/encryption/in-transit/app_service_ftps_unused/main.tf:36

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/best-practices/webapp_php_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/iam/webapp_client_cert_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

test-cases/terraform/azure/best-practices/webapp_lin_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].https_only' is set

Workspaces Workspace Volume Not Encrypted

Results 4

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

AWS Workspaces Workspace data stored in volumes should be encrypted

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:84

Expected: aws_workspaces_workspace.root_volume_encryption_enabled is set to true

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:84

Expected: aws_workspaces_workspace.root_volume_encryption_enabled is set to true

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:83

Expected: aws_workspaces_workspace.user_volume_encryption_enabled is set to true

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:83

Expected: aws_workspaces_workspace.user_volume_encryption_enabled is set to true

ALB Is Not Integrated With WAF

Results 5

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

All Application Load Balancers (ALB) must be protected with Web Application Firewall (WAF) service

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:48

Expected: 'aws_alb[disabled]' is not 'internal' and has a 'aws_wafregional_web_acl_association' associated

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:32

Expected: 'aws_alb[default]' is not 'internal' and has a 'aws_wafregional_web_acl_association' associated

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: 'aws_lb[default]' is not 'internal' and has a 'aws_wafregional_web_acl_association' associated

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:60

Expected: 'aws_lb[alb_test]' is not 'internal' and has a 'aws_wafregional_web_acl_association' associated

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:39

Expected: 'aws_lb[disabled]' is not 'internal' and has a 'aws_wafregional_web_acl_association' associated

ALB Not Dropping Invalid Headers

Results **6**

Severity	MEDIUM
Platform	Terraform
Category	Best Practices

Description

It's considered a best practice when using Application Load Balancers to drop invalid header fields

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:54

Expected: aws_alb[{{disabled}}].drop_invalid_header_fields is set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: aws_lb[{{default}}].drop_invalid_header_fields is set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:32

Expected: aws_alb[{{default}}].drop_invalid_header_fields is set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:45

Expected: aws_lb[{{disabled}}].drop_invalid_header_fields is set to true

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:60

Expected: aws_lb[{{alb_test}}].drop_invalid_header_fields is set to true

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:49

Expected: aws_lb[{{test}}].drop_invalid_header_fields is set to true

API Gateway Deployment Without Access Log Setting

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

API Gateway Deployment should have access log setting defined when connected to an API Gateway Stage.

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:38

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

API Gateway Method Does Not Contains An API Key

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

An API Key should be required on a method request.

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:22

Expected: resource.aws_api_gateway_method[api_gw_method].api_key_required is defined

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:22

Expected: resource.aws_api_gateway_method[api_gw_method].api_key_required is defined

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:22

Expected: resource.aws_api_gateway_method[api_gw_method].api_key_required is defined

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:50

Expected: resource.aws_api_gateway_method[api_gw_method].api_key_required is defined

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:22

Expected: resource.aws_api_gateway_method[api_gw_method].api_key_required is defined

API Gateway With CloudWatch Logging Disabled

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

AWS CloudWatch Logs for APIs is not enabled

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: 'aws_cloudwatch_log_group' is set

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: 'aws_cloudwatch_log_group' is set

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: 'aws_cloudwatch_log_group' is set

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: 'aws_cloudwatch_log_group' is set

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: 'aws_cloudwatch_log_group' is set

API Gateway With Open Access

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

API Gateway Method should restrict the authorization type, except for the HTTP OPTIONS method.

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:25

Expected: aws_api_gateway_method.authorization is only 'NONE' if http_method is 'OPTIONS'

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:25

Expected: aws_api_gateway_method.authorization is only 'NONE' if http_method is 'OPTIONS'

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:53

Expected: aws_api_gateway_method.authorization is only 'NONE' if http_method is 'OPTIONS'

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:25

Expected: aws_api_gateway_method.authorization is only 'NONE' if http_method is 'OPTIONS'

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:25

Expected: aws_api_gateway_method.authorization is only 'NONE' if http_method is 'OPTIONS'

API Gateway Without Configured Authorizer

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

API Gateway REST API should have an API Gateway Authorizer

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:5

Expected: API Gateway REST API is associated with an API Gateway Authorizer

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:5

Expected: API Gateway REST API is associated with an API Gateway Authorizer

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:5

Expected: API Gateway REST API is associated with an API Gateway Authorizer

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:5

Expected: API Gateway REST API is associated with an API Gateway Authorizer

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:5

Expected: API Gateway REST API is associated with an API Gateway Authorizer

API Gateway Without Content Encoding

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Enable Content Encoding through the attribute 'minimum_compression_size'. This value should be greater than -1 and smaller than 10485760

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:5

Expected: Attribute 'minimum_compression_size' is set, greater than -1 and smaller than 10485760

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:5

Expected: Attribute 'minimum_compression_size' is set, greater than -1 and smaller than 10485760

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:5

Expected: Attribute 'minimum_compression_size' is set, greater than -1 and smaller than 10485760

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:5

Expected: Attribute 'minimum_compression_size' is set, greater than -1 and smaller than 10485760

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:5

Expected: Attribute 'minimum_compression_size' is set, greater than -1 and smaller than 10485760

Checkmarx

KICS REPORT vv1.5.2

API Gateway Without SSL Certificate

Results 5

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

SSL Client Certificate should be enabled in aws_api_gateway_stage resource

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: Attribute 'client_certificate_id' is set

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: Attribute 'client_certificate_id' is set

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: Attribute 'client_certificate_id' is set

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: Attribute 'client_certificate_id' is set

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: Attribute 'client_certificate_id' is set

API Gateway X-Ray Disabled

Results 5

Severity MEDIUM
Platform Terraform
Category Observability

Description

X-ray Tracing is not enabled

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: 'aws_api_gateway_stage[api_gw_stage].xray_tracing_enabled' is set

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: 'aws_api_gateway_stage[api_gw_stage].xray_tracing_enabled' is set

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: 'aws_api_gateway_stage[api_gw_stage].xray_tracing_enabled' is set

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: 'aws_api_gateway_stage[api_gw_stage].xray_tracing_enabled' is set

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: 'aws_api_gateway_stage[api_gw_stage].xray_tracing_enabled' is set

API Gateway without WAF

Results 5

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

API Gateway should have WAF (Web Application Firewall) enabled

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: API Gateway Stage is associated with a Web Application Firewall

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: API Gateway Stage is associated with a Web Application Firewall

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: API Gateway Stage is associated with a Web Application Firewall

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: API Gateway Stage is associated with a Web Application Firewall

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: API Gateway Stage is associated with a Web Application Firewall

Api Gateway Access Logging Disabled

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

RDS does not have any kind of logger

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: 'access_log_settings' is defined

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: 'access_log_settings' is defined

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: 'access_log_settings' is defined

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: 'access_log_settings' is defined

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: 'access_log_settings' is defined

Azure Cognitive Search Public Network Access Enabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

Public Network Access should be disabled for Azure Cognitive Search

test-cases/terraform/azure/logging/search_diagnostic_not_enabled/main.tf:15

Expected: 'azurerm_search_service[search].public_network_access_enabled' is defined and set to false

CloudTrail Multi Region Disabled

Results **6**

Severity	MEDIUM
Platform	Terraform
Category	Observability
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 3.1
Title	Ensure CloudTrail is enabled in all regions

Description

Checkmarx

KICS REPORT vv1.5.2

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. CloudTrail provides a history of AWS API calls for an account, including API calls made via the Management Console, SDKs, command line tools, and higher-level AWS services (such as CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing. Additionally, ensuring that a multi-regions trail exists will ensure that unexpected activity occurring in otherwise unused regions is detected ensuring that a multi-regions trail exists will ensure that Global Service Logging is enabled for a trail by default to capture recording of events generated onAWS global services for a multi-regions trail, ensuring that management events configured for all type of Read/Writes ensures recording of management operations that are performed on all resources in an AWS account

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: aws_cloudtrail[foobar].is_multi_region_trail is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:7

Expected: aws_cloudtrail[foobar].include_global_service_events undefined or is set to true

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:15

Expected: aws_cloudtrail[foobar].include_global_service_events undefined or is set to true

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: aws_cloudtrail[foobar].is_multi_region_trail is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: aws_cloudtrail[foobar].is_multi_region_trail is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:15

Expected: aws_cloudtrail[foobar].include_global_service_events undefined or is set to true

CloudTrail Not Integrated With CloudWatch

Results **6**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

CloudTrail should be integrated with CloudWatch

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: aws_cloudtrail[foobar].cloud_watch_logs_group_arn is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: aws_cloudtrail[foobar].cloud_watch_logs_role_arn is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: aws_cloudtrail[foobar].cloud_watch_logs_group_arn is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: aws_cloudtrail[foobar].cloud_watch_logs_group_arn is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: aws_cloudtrail[foobar].cloud_watch_logs_role_arn is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: aws_cloudtrail[foobar].cloud_watch_logs_role_arn is defined and not null

Checkmarx

KICS REPORT vv1.5.2

CloudTrail SNS Topic Name Undefined

Results 3

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Check if SNS topic name is set for CloudTrail

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: 'aws_cloudtrail[foobar].sns_topic_name' is set and is not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: 'aws_cloudtrail[foobar].sns_topic_name' is set and is not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: 'aws_cloudtrail[foobar].sns_topic_name' is set and is not null

CloudWatch Logs Destination With Vulnerable Policy

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

CloudWatch Logs destination policy should avoid wildcard in 'principals' and 'actions'

test-cases/terraform/aws/iam/resource-policies/cloudwatch_log_destination_insecure_policy/main.tf:87

Expected: aws_cloudwatch_log_destination_policy[test_destination_policy].access_policy does not have wildcard in 'principals' and 'actions'

CloudWatch Metrics Disabled

Results 5

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Checks if CloudWatch Metrics is Enabled

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:55

Expected: aws_api_gateway_method_settings[api_gw_method_sett].settings.metrics_enabled is defined and not null

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:83

Expected: aws_api_gateway_method_settings[api_gw_method_sett].settings.metrics_enabled is defined and not null

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:55

Expected: aws_api_gateway_method_settings[api_gw_method_sett].settings.metrics_enabled is defined and not null

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:55

Expected: aws_api_gateway_method_settings[api_gw_method_sett].settings.metrics_enabled is defined and not null

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:55

Expected: aws_api_gateway_method_settings[api_gw_method_sett].settings.metrics_enabled is defined and not null

CloudWatch Without Retention Period Specified

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

AWS CloudWatch Log groups should have retention days specified

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/logging/cloudwatch_log_groups_no_retention/main.tf:5

Expected: Attribute 'retention_in_days' is set and valid

Cloudfront Logging Disabled

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

AWS Cloudfront distributions must be have logging enabled, which means the attribute 'logging_config' must be defined

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:44

Expected: aws_cloudfront_distribution[s3_distribution].logging_config is defined

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:14

Expected: aws_cloudfront_distribution[s3_distribution].logging_config is defined

DOCDB Cluster Encrypted With AWS Managed Key

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

DOCDB Cluster should be encrypted with customer-managed KMS keys instead of AWS managed keys

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_at_rest_using_cmk_not_customer_managed/main.tf:16

Expected: DOCDB Cluster is not encrypted with AWS managed key

Default VPC Exists

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

It isn't recommended to use resources in default VPC

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:12

Expected: 'aws_default_vpc' should not exist

DynamoDB Table Not Encrypted

Results **4**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

AWS DynamoDB Tables should have server-side encryption

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:90

Expected: aws_dynamodb_table.server_side_encryption.enabled is set to true

test-cases/terraform/aws/encryption/at-rest/dynamodb_not_encrypted/main.tf:1

Expected: aws_dynamodb_table.server_side_encryption.enabled is set to true

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:143

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_dynamodb_table.server_side_encryption.enabled is set to true

test-cases/terraform/aws/best-practices/dynamodb_without_recovery_enabled/main.tf:1

Expected: aws_dynamodb_table.server_side_encryption.enabled is set to true

EBS Volume Encryption Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.2.1
Title	Ensure EBS volume encryption is enabled

Description

Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service. While disabled by default, forcing encryption at EBS volume creation is supported. Encrypting data at rest reduces the likelihood that it is unintentionally exposed and can nullify the impact of disclosure if the encryption remains unbroken.

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:15

Expected: One of 'aws_ebs_volume.encrypted' is defined

ECR Image Tag Not Immutable

Results 3

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

ECR should have an image tag be immutable

test-cases/terraform/aws/iam/resource-policies/ecr_not_secure_policy/main.tf:3

Expected: aws_ecr_repository.foo.image_tag_mutability is 'IMMUTABLE'

test-cases/terraform/aws/best-practices/ecr_make_tags_immutable/main.tf:3

Expected: aws_ecr_repository.foo.image_tag_mutability is 'IMMUTABLE'

test-cases/terraform/aws/best-practices/ecr_use_image_scanning/main.tf:3

Expected: aws_ecr_repository.foo.image_tag_mutability is 'IMMUTABLE'

ECR Repository Not Encrypted

Results 4

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

ECR (Elastic Container Registry) Repository encryption should be set

test-cases/terraform/aws/best-practices/ecr_make_tags_immutable/main.tf:1

Expected: The attribute 'encryption_configuration' is defined and not null

test-cases/terraform/aws/best-practices/ecr_use_image_scanning/main.tf:1

Expected: The attribute 'encryption_configuration' is defined and not null

test-cases/terraform/aws/iam/resource-policies/ecr_not_secure_policy/main.tf:1

Expected: The attribute 'encryption_configuration' is defined and not null

test-cases/terraform/aws/encryption/at-rest/ecr_repo_not_encrypted/main.tf:1

Expected: The attribute 'encryption_configuration' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

ElastiCache Redis Cluster Without Backup

Results 2

Severity MEDIUM
Platform Terraform
Category Backup

Description

ElastiCache Redis cluster should have 'snapshot_retention_limit' higher than 0

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:1

Expected: 'snapshot_retention_limit' is higher than 0

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:16

Expected: 'snapshot_retention_limit' is higher than 0

ElastiCache Replication Group Not Encrypted At Rest

Results 2

Severity MEDIUM
Platform Terraform
Category Encryption

Description

ElastiCache Replication Group encryption should be enabled at Rest

test-cases/terraform/aws/encryption/at-rest/elasticache_replication_group_not_encrypted_at_rest/main.tf:1

Expected: The attribute 'at_rest_encryption_enabled' is set to true

test-cases/terraform/aws/encryption/in-transit/elasticache_replication_group_not_encrypted_in_transit/main.tf:5

Expected: The attribute 'at_rest_encryption_enabled' is set to true

ElastiCache Replication Group Not Encrypted At Transit

Results 2

Severity MEDIUM
Platform Terraform
Category Encryption

Description

ElastiCache Replication Group encryption should be enabled at Transit

test-cases/terraform/aws/encryption/in-transit/elasticache_replication_group_not_encrypted_in_transit/main.tf:5

Expected: The attribute 'transit_encryption_enabled' is set to true

test-cases/terraform/aws/encryption/at-rest/elasticache_replication_group_not_encrypted_at_rest/main.tf:1

Expected: The attribute 'transit_encryption_enabled' is set to true

ElasticSearch Not Encrypted At Rest

Results 5

Severity MEDIUM
Platform Terraform
Category Encryption

Description

Check if ElasticSearch encryption is disabled at Rest

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:107

Expected: 'encrypt_at_rest' is set and enabled

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: 'encrypt_at_rest' is set and enabled

test-cases/terraform/aws/encryption/at-rest/elasticsearch_not_encrypted/main.tf:1

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Expected: 'encrypt_at_rest' is set and enabled

test-cases/terraform/aws/encryption/in-transit/elasticsearch_encrypt_node_to_node_disabled/main.tf:5

Expected: 'encrypt_at_rest' is set and enabled

test-cases/terraform/aws/logging/elasticsearch_domain_logging_disabled/main.tf:1

Expected: 'encrypt_at_rest' is set and enabled

Elasticsearch Domain Not Encrypted Node To Node

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Elasticsearch Domain encryption should be enabled node to node

test-cases/terraform/aws/logging/elasticsearch_domain_logging_disabled/main.tf:1

Expected: The attribute 'node_to_node_encryption' is set to true

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:107

Expected: The attribute 'node_to_node_encryption' is set to true

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: The attribute 'node_to_node_encryption' is set to true

test-cases/terraform/aws/encryption/at-rest/elasticsearch_not_encrypted/main.tf:1

Expected: The attribute 'node_to_node_encryption' is set to true

test-cases/terraform/aws/encryption/in-transit/elasticsearch_encrypt_node_to_node_disabled/main.tf:5

Expected: The attribute 'node_to_node_encryption' is set to true

Elasticsearch Domain With Vulnerable Policy

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Elasticsearch Domain policy should avoid wildcard in 'Action' and 'Principal'.

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:18

Expected: aws_elasticsearch_domain_policy[main].access_policies does not have wildcard in 'Action' and 'Principal'

Elasticsearch Log is disabled

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

AWS Elasticsearch should have logs enabled

test-cases/terraform/aws/encryption/in-transit/elasticsearch_encrypt_node_to_node_disabled/main.tf:5

Expected: 'log_publishing_options' is defined and not null

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: 'log_publishing_options' is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:107

Expected: 'log_publishing_options' is defined and not null

test-cases/terraform/aws/logging/elasticsearch_domain_logging_disabled/main.tf:1

Checkmarx

KICS REPORT vv1.5.2

Expected: 'log_publishing_options' is defined and not null

test-cases/terraform/aws/encryption/at-rest/elasticsearch_not_encrypted/main.tf:1

Expected: 'log_publishing_options' is defined and not null

Elasticsearch Without IAM Authentication

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

AWS Elasticsearch should ensure IAM Authentication

test-cases/terraform/aws/encryption/at-rest/elasticsearch_not_encrypted/main.tf:1

Expected: Elasticsearch Domain has a policy associated

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: Elasticsearch Domain ensure IAM Authentication

test-cases/terraform/aws/logging/elasticsearch_domain_logging_disabled/main.tf:1

Expected: Elasticsearch Domain has a policy associated

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:107

Expected: Elasticsearch Domain has a policy associated

test-cases/terraform/aws/encryption/in-transit/elasticsearch_encrypt_node_to_node_disabled/main.tf:5

Expected: Elasticsearch Domain has a policy associated

Email Alerts Disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Make sure that alerts notifications are set to 'On' in the Azure Security Center Contact

test-cases/terraform/azure/best-practices/email_notifications_for_high_severity_alerts_not_used/main.tf:22

Expected: 'azurerm_security_center_contact.example.alert_notifications' is true

Function App Client Certificates Unrequired

Results **9**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Azure Function App should have 'client_cert_mode' set to required

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:46

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/iam/func_app_authentication/main.tf:42

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:50

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is set to 'Required'

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:35

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:35

Checkmarx

KICS REPORT vv1.5.2

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:28

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:35

Expected: 'azurerm_function_app[functionapp].client_cert_mode' is defined and not null

Function App Managed Identity Disabled

Results **9**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Azure Function App should have managed identity enabled

test-cases/terraform/azure/iam/func_app_authentication/main.tf:42

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:35

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:46

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:35

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:37

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:43

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:35

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:28

Expected: 'azurerm_function_app[functionapp].identity' is defined and not null

Glue With Vulnerable Policy

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Glue policy should avoid wildcard in 'principals' and 'actions'

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:68

Expected: aws_glue_resource_policy[example].policy does not have wildcard in 'principals' and 'actions'

IAM Access Analyzer Undefined

Results **1**

Checkmarx

KICS REPORT vv1.5.2

Severity MEDIUM
Platform Terraform
Category Access Control

Description

IAM Access Analyzer should be defined to identify unintentional access

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: 'aws_accessanalyzer_analyzer' is set

IAM Policy Grants Full Permissions

Results **5**

Severity MEDIUM
Platform Terraform
Category Access Control

Description

IAM policies allow all ('*') in a statement action

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:49

Expected: 'policy.Statement.Resource' not equal '*'

test-cases/terraform/aws/iam/iam-entities/iam_user_inline_policy_attach/main.tf:13

Expected: 'policy.Statement.Resource' not equal '*'

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:81

Expected: 'policy.Statement.Resource' not equal '*'

test-cases/terraform/aws/iam/iam-entities/policy-too-broad/main.tf:26

Expected: 'policy.Statement.Resource' not equal '*'

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:29

Expected: 'policy.Statement.Resource' not equal '*'

IAM Role Policy passRole Allows All

Results **1**

Severity MEDIUM
Platform Terraform
Category Access Control

Description

Using the iam:passrole action with wildcards (*) in the resource can be overly permissive because it allows iam:passrole permissions on multiple resources

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:29

Expected: 'aws_iam_role_policy.policy.Statement.Action' iam:passrole doesn't have Resource '*'

IAM User With Access To Console

Results **6**

Severity MEDIUM
Platform Terraform
Category Access Control

Description

AWS IAM Users should not have access to console

test-cases/terraform/hcl_language_complexity/using_count_and_ternary_expr/main.tf:23

Expected: aws_iam_user.jill.name doesn't have aws_iam_user_login_profile

test-cases/terraform/hcl_language_complexity/using_for_each/main.tf:10

Expected: each.value doesn't have aws_iam_user_login_profile

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/hcl_language_complexity/using_locals/main.tf:12

Expected: local.user_name doesn't have aws_iam_user_login_profile

test-cases/terraform/aws/iam/iam-entities/human_users_defined/main.tf:6

Expected: aws_iam_user.iam_user_1.name doesn't have aws_iam_user_login_profile

test-cases/terraform/hcl_language_complexity/using_module_multi/mymodule/user.tf:21

Expected: aws_iam_user.user.name doesn't have aws_iam_user_login_profile

test-cases/terraform/hcl_language_complexity/using_count_and_ternary_expr/main.tf:11

Expected: aws_iam_user.jack.name doesn't have aws_iam_user_login_profile

Instance With No VPC

Results **10**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Instance should be configured in VPC (Virtual Private Cloud)

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:31

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/logging/ec2_without_monitoring/main.tf:17

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:98

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:45

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:80

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:106

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:98

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/ec2_ebs_not_optimized/main.tf:17

Expected: Attribute 'vpc_security_group_ids' is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:93

Expected: Attribute 'vpc_security_group_ids' is defined and not null

Lambda Function Without Tags

Results **4**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

AWS Lambda Functions must have associated tags.

test-cases/terraform/aws/logging/lambda_without_xray/main.tf:21

Expected: aws_lambda_function[test_lambda].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_lambda_function[my-lambda].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_explicit_log_group/main.tf:57

Expected: aws_lambda_function[test_lambda].tags is defined and not null

test-cases/terraform/aws/networking/lambda_not_in_vpc/main.tf:21

Expected: aws_lambda_function[test_lambda].tags is defined and not null

Lambda With Vulnerable Policy

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

The attribute 'action' should not have wildcard

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:35

Expected: aws_lambda_permission[all].action does not have wildcard

MSSQL Server Auditing Disabled

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Make sure that for MSSQL Servers, that 'Auditing' is set to 'On'

test-cases/terraform/azure/logging/sql_server_audit_not_used/main.tf:17

Expected: 'azurerm_mssql_server.sql.extended_auditing_policy' exists

test-cases/terraform/azure/iam/sql-server-ad-admin-not-set/main.tf:17

Expected: 'azurerm_mssql_server.sql.extended_auditing_policy' exists

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:21

Expected: 'azurerm_mssql_server.my-sql-server.extended_auditing_policy' exists

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:25

Expected: 'azurerm_mssql_server.sql.extended_auditing_policy' exists

test-cases/terraform/azure/encryption/at-rest/sql_encryption_customer_key_not_set/main.tf:15

Expected: 'azurerm_mssql_server.sql.extended_auditing_policy' exists

Neptune Cluster With IAM Database Authentication Disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Neptune Cluster should have IAM Database Authentication enabled

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:66

Expected: 'iam_database_authentication_enabled' is set to true

Neptune Database Cluster Encryption Disabled

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Check if Neptune Cluster Storage is securely encrypted

test-cases/terraform/aws/logging/neptune_cluster_no_logging/main.tf:1

Expected: 'storage_encrypted' should be set with value true

test-cases/terraform/aws/encryption/at-rest/neptune_cluster_no_encryption/main.tf:1

Expected: 'storage_encrypted' should be set with value true

Policy Without Principal

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

All policies, except IAM identity-based policies, should have the 'Principal' element defined

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:68

Expected: 'Principal' is set

test-cases/terraform/aws/iam/iam-entities/policy_missing_principal/main.tf:9

Expected: 'Principal' is set

PostgreSQL Log Checkpoints Disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Make sure that for Postgre SQL Database Server, parameter 'log_checkpoints' is set to 'ON'

test-cases/terraform/azure/logging/postgresql_logcheckpoints_not_enabled/main.tf:33

Expected: 'azurerm_postgresql_configuration.example.value' should be 'ON'

PostgreSQL Log Connections Not Set

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Make sure that for PostgreSQL Database, server parameter 'log_connections' is set to 'ON'

test-cases/terraform/azure/logging/postgresql_log_connections_not_enabled/main.tf:33

Expected: 'azurerm_postgresql_configuration.example.value' is 'ON'

PostgreSQL Log Disconnections Not Set

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

Make sure that for PostgreSQL Database, server parameter 'log_disconnections' is set to 'ON'

test-cases/terraform/azure/logging/postgresql_log_disconnections_not_enabled/main.tf:33

Expected: 'azurerm_postgresql_configuration.example.value' is 'ON'

Checkmarx

KICS REPORT vv1.5.2

Public and Private EC2 Share Role

Results 1

Severity MEDIUM
Platform Terraform
Category Access Control

Description

Public and private EC2 istances should not share the same role.

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:102

Expected: Public and private instances do not share the same role

RDS Cluster With Backup Disabled

Results 2

Severity MEDIUM
Platform Terraform
Category Best Practices

Description

RDS Cluster backup retention period should be specifically defined

test-cases/terraform/aws/best-practices/rds_retention_period_set/main.tf:1

Expected: aws_rds_cluster.backup_retention_period is defined and not null

test-cases/terraform/aws/encryption/at-rest/rds_cluster_encrypt_at_rest_disabled/main.tf:5

Expected: aws_rds_cluster.backup_retention_period is defined and not null

RDS With Backup Disabled

Results 4

Severity MEDIUM
Platform Terraform
Category Backup

Description

RDS configured without backup

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:113

Expected: 'backup_retention_period' exists

test-cases/terraform/aws/logging/rds_without_logging/main.tf:1

Expected: 'backup_retention_period' exists

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:60

Expected: 'backup_retention_period' exists

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:1

Expected: 'backup_retention_period' exists

Redshift Cluster Logging Disabled

Results 4

Severity MEDIUM
Platform Terraform
Category Observability

Description

Make sure Logging is enabled for Redshift Cluster

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: 'aws_redshift_cluster.logging' is true

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: 'aws_redshift_cluster.logging' is true

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:103

Expected: 'aws_redshift_cluster.logging' is true

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: 'aws_redshift_cluster.logging' is true

Redshift Cluster Without VPC

Results **6**

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Redshift Cluster should be configured in VPC (Virtual Private Cloud)

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster[default].cluster_subnet_group_name is set

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster[default].vpc_security_group_ids is set

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Expected: aws_redshift_cluster[test].vpc_security_group_ids is set

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster[default].vpc_security_group_ids is set

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster[default].cluster_subnet_group_name is set

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Expected: aws_redshift_cluster[test].cluster_subnet_group_name is set

Role Definition Allows Custom Role Creation

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Role Definition should not allow custom role creation

test-cases/terraform/azure/iam/custom-role-owner-exists/main.tf:24

Expected: azurerm_role_definition[example].permissions.actions does not allow custom role creation

S3 Bucket Policy Accepts HTTP Requests

Results **5**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

S3 Bucket policy should not accept HTTP Requests

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:22

Expected: aws_s3_bucket[foo].policy does not accept HTTP Requests

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:14

Expected: aws_s3_bucket[foo].policy does not accept HTTP Requests

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:22

Expected: aws_s3_bucket[foo].policy does not accept HTTP Requests

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:12

Expected: aws_s3_bucket_policy[bucket_2_policy].policy does not accept HTTP Requests

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:13

Expected: aws_s3_bucket[cdn-content].policy does not accept HTTP Requests

S3 Bucket Without Versioning

Results **19**

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

S3 bucket should have versioning enabled

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:32

Expected: 'versioning' is set to true

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:1

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/s3_bucket_non_encrypted/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/logging/s3_access_logging_disabled/main.tf:1

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:33

Expected: 'versioning' is set to true

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:1

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: 'versioning' is set to true

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:1

Expected: 'versioning' is set to true

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: 'versioning' is set to true

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: 'versioning' is set to true

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:14

Checkmarx

KICS REPORT vv1.5.2

Expected: 'versioning' is set to true

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Expected: 'versioning' is set to true

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: 'versioning' is set to true

SNS Topic Encrypted With AWS Managed Key

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

SNS (Simple Notification Service) Topic should be encrypted with customer-managed KMS keys instead of AWS managed keys

test-cases/terraform/aws/encryption/at-rest/sns_topic_encrypted_at_rest_with_aws_managed_key_by_key_arn/main.tf:11

Expected: SNS Topic is not encrypted with AWS managed key

SNS Topic Not Encrypted

Results **3**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

SNS (Simple Notification Service) Topic should be encrypted

test-cases/terraform/aws/iam/resource-policies/glacier_vault_not_secure_policy/main.tf:5

Expected: SNS Topic is encrypted

test-cases/terraform/aws/best-practices/tag_all_items/main.tf:5

Expected: SNS Topic is encrypted

test-cases/terraform/aws/best-practices/tag_all_items/plan.json:8

Expected: SNS Topic is encrypted

SQL Analysis Services Port 2383 (TCP) Is Publicly Accessible

Results **3**

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

Check if port 2383 on TCP is publicly accessible by checking the CIDR block range that can access it.

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: aws_security_group doesn't openSQL Analysis Services Port 2383

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: aws_security_group doesn't openSQL Analysis Services Port 2383

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: aws_security_group doesn't openSQL Analysis Services Port 2383

SQL Server Auditing Disabled

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Observability

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Description

Make sure that for SQL Servers, 'Auditing' is set to 'On'

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:15

Expected: 'azurerm_sql_server.sql.extended_auditing_policy' exists

test-cases/terraform/azure/best-practices/sql_vulnerability_assessment_not_enabled/main.tf:15

Expected: 'azurerm_sql_server.sql.extended_auditing_policy' exists

SQS VPC Endpoint Without DNS Resolution

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

SQS VPC Endpoint should have DNS resolution enabled

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:95

Expected: 'enable_dns_support' is set to true or undefined

Secrets Manager With Vulnerable Policy

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Secrets Manager policy should avoid wildcard in 'Principal' and 'Action'

test-cases/terraform/aws/iam/resource-policies/secrets_manager_not_secure_policy/main.tf:12

Expected: aws_secretsmanager_secret_policy[example].policy does not have wildcard in 'Principal' and 'Action'

Secretsmanager Secret Encrypted With AWS Managed Key

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Secrets Manager secret should be encrypted with customer-managed KMS keys instead of AWS managed keys

test-cases/terraform/aws/encryption/at-rest/secretsmanager_secrets_encrypted_at_rest_with_aws_managed_key_by_key_arn/main.tf:11

Expected: Secrets Manager secret is not encrypted with AWS managed key

Secretsmanager Secret Without KMS

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

AWS Secretmanager should use AWS KMS customer master key (CMK) to encrypt the secret values in the versions stored in the secret

test-cases/terraform/aws/iam/resource-policies/secrets_manager_not_secure_policy/main.tf:5

Expected: aws_secretsmanager_secret.kms_key_id is defined and not null

test-cases/terraform/aws/encryption/at-rest/secretsmanager_secrets_encrypted_at_rest_with_aws_managed_key_by_default/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_secretsmanager_secret.kms_key_id is defined and not null

Security Center Pricing Tier Is Not Standard

Results 7

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Make sure that the 'Standard' pricing tiers were selected.

test-cases/terraform/azure/best-practices/defender_for_sql_servers_not_used/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_app_services_disabled/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_kubernetes_not_used/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_servers_not_used/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_storage_not_used/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_keyvault_disabled/main.tf:11

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

test-cases/terraform/azure/best-practices/defender_for_container_registry_not_used/main.tf:19

Expected: 'azurerm_security_center_subscription_pricing.example.tier' is 'Standard'

Sensitive Port Is Exposed To Wide Private Network

Results 2

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

A sensitive port, such as port 23 or port 110, is open for a wide private network in either TCP or UDP protocol

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:19

Expected: HTTPS (TCP:443) should not be allowed

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:19

Expected: HTTPS (TCP:443) should not be allowed

Storage Account Not Using Latest TLS Encryption Version

Results 20

Severity MEDIUM
Platform Terraform
Category Encryption

Description

Ensure Storage Account is using the latest version of TLS encryption

test-cases/terraform/azure/logging/vmss_win_diagnostic_log_disabled/main.tf:41

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:24

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:35

Expected: 'azurerm_storage_account[my-storage-account].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/encryption/at-rest/activitylog_storage_account_encryption_not_enabled/main.tf:18

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:24

Expected: 'azurerm_storage_account[example].min_tls_version' is defined and not null

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:23

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/encryption/at-rest/storacc_encryption_not_enabled/main.tf:18

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:11

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/logging/iot_hub_diagnostic_not_enabled/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/logging/batch_diagnostic_disabled/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/iam/storage_account_public_access_disabled/main.tf:16

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/logging/sql-server-audit-retention-30/main.tf:17

Expected: 'azurerm_storage_account[example].min_tls_version' is defined and not null

test-cases/terraform/azure/iam/func_app_authentication/main.tf:22

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/vm_unmanaged_disks/main.tf:42

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:15

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:41

Expected: 'azurerm_storage_account[storacc].min_tls_version' is defined and not null

Unscanned ECR Image

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Checks if the ECR Image has been scanned

test-cases/terraform/aws/best-practices/ecr_use_image_scanning/main.tf:6

Expected: aws_ecr_repository[foo].image_scanning_configuration.scan_on_push is true

Checkmarx

KICS REPORT vv1.5.2

VPC FlowLogs Disabled

Results 19

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

VPC hasn't got any FlowLog associated

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:10

Expected: aws_vpc[vpc] is the same as Flow Logs VPC id

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:26

Expected: aws_vpc[vpc1] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:10

Expected: aws_vpc[nondefault] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:35

Expected: aws_vpc[vpc2] is the same as Flow Logs VPC id

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:10

Expected: aws_vpc[vpc] is the same as Flow Logs VPC id

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:3

Expected: aws_vpc[example] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:20

Expected: aws_vpc[vpc1] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:10

Expected: aws_vpc[nondefault] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:14

Expected: aws_vpc[vpc] is the same as Flow Logs VPC id

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:1

Expected: vpc.enable_flow_log is set to true

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:5

Expected: aws_vpc[main] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:5

Expected: aws_vpc[external] is the same as Flow Logs VPC id

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:10

Expected: aws_vpc[vpc] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:5

Expected: aws_vpc[nondefault] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:12

Expected: aws_vpc[main] is the same as Flow Logs VPC id

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:5

Expected: aws_vpc[vpc1] is the same as Flow Logs VPC id

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:5

Expected: aws_vpc[nondefault] is the same as Flow Logs VPC id

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:10

Expected: vpc.enable_flow_log is set to true

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:8

Expected: aws_vpc[main] is the same as Flow Logs VPC id

Checkmarx

KICS REPORT vv1.5.2

VPC Subnet Assigns Public IP

Results 3

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

VPC Subnet should not assign public IP

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:13

Expected: aws_subnet[public-subnet].map_public_ip_on_launch is set to false or undefined

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:10

Expected: vpc.map_public_ip_on_launch is set to false

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:1

Expected: vpc.map_public_ip_on_launch is set to false

VPC Without Network Firewall

Results 17

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

VPC should have a Network Firewall associated

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:5

Expected: aws_vpc[nondefault] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:5

Expected: aws_vpc[main] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:10

Expected: aws_vpc[vpc] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:3

Expected: aws_vpc[example] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:12

Expected: aws_vpc[main] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:14

Expected: aws_vpc[vpc] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:10

Expected: aws_vpc[nondefault] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:10

Expected: aws_vpc[nondefault] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:5

Expected: aws_vpc[nondefault] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:10

Expected: aws_vpc[vpc] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:20

Expected: aws_vpc[vpc1] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:5

Expected: aws_vpc[external] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_vpc[vpc1] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:35

Expected: aws_vpc[vpc2] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:8

Expected: aws_vpc[main] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:26

Expected: aws_vpc[vpc1] has an 'aws_networkfirewall_firewall' associated

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:10

Expected: aws_vpc[vpc] has an 'aws_networkfirewall_firewall' associated

Virtual Network with DDoS Protection Plan disabled

Results **7**

Severity	MEDIUM
Platform	Terraform
Category	Availability

Description

Virtual Network should have DDoS Protection Plan enabled

test-cases/terraform/azure/best-practices/vpn_gw_using_basic_sku/main.tf:23

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/networking/vm_public_rdp_nat_opened/main.tf:17

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/logging/vmss_win_diagnostic_log_disabled/main.tf:15

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/best-practices/vm_unmanaged_disks/main.tf:16

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/networking/vmss_public_rdp_lb_opened/main.tf:17

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/best-practices/vmss_unmanaged_disks/main.tf:15

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

test-cases/terraform/azure/networking/vm_public_rdp_lb_opened/main.tf:17

Expected: 'azurerm_virtual_network[vnet].ddos_protection_plan' is defined and not null

ALB Deletion Protection Disabled

Results **6**

Severity	LOW
Platform	Terraform
Category	Insecure Configurations

Description

Application Load Balancer should have deletion protection enabled

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:32

Expected: 'enable_deletion_protection' is defined and set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:39

Expected: 'enable_deletion_protection' is defined and set to true

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:49

Expected: 'enable_deletion_protection' is defined and set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: 'enable_deletion_protection' is defined and set to true

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:60

Expected: 'enable_deletion_protection' is defined and set to true

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:48

Expected: 'enable_deletion_protection' is defined and set to true

API Gateway Deployment Without API Gateway UsagePlan Associated

Results **5**

Severity	LOW
Platform	Terraform
Category	Observability

Description

API Gateway Deployment should have API Gateway UsagePlan defined and associated.

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:38

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:10

Expected: aws_api_gateway_deployment[api_gw_deploy] has a 'aws_api_gateway_usage_plan' resource associated.

API Gateway Stage Without API Gateway UsagePlan Associated

Results **5**

Severity	LOW
Platform	Terraform
Category	Resource Management

Description

API Gateway Stage should have API Gateway UsagePlan defined and associated.

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: aws_api_gateway_stage[api_gw_stage] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: aws_api_gateway_stage[api_gw_stage] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: aws_api_gateway_stage[api_gw_stage] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: aws_api_gateway_stage[api_gw_stage] has a 'aws_api_gateway_usage_plan' resource associated.

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: aws_api_gateway_stage[api_gw_stage] has a 'aws_api_gateway_usage_plan' resource associated.

App Service HTTP2 Disabled

Results **9**

Severity	LOW
Platform	Terraform
Category	Insecure Configurations

Description

App Service should have 'http2_enabled' enabled

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/azure/encryption/in-transit/app_service_ftps_unused/main.tf:42

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/best-practices/webapp_php_isnot_latest/main.tf:34

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:34

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/iam/app_service_authentication_missing/main.tf:28

Expected: 'azurerm_app_service[webapp].site_config' is defined and not null

test-cases/terraform/azure/best-practices/webapp_http2_not_enabled/main.tf:36

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is set to true

test-cases/terraform/azure/iam/webapp_client_cert_not_enabled/main.tf:35

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/best-practices/webapp_lin_java_isnot_latest/main.tf:38

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/best-practices/webapp_win_java_isnot_latest/main.tf:38

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/iam/webapp_not_use_managedidentity/main.tf:34

Expected: 'azurerm_app_service[webapp].site_config.http2_enabled' is defined and not null

CloudTrail Log File Validation Disabled

Results **3**

Severity	LOW
Platform	Terraform
Category	Observability
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 3.2
Title	Ensure CloudTrail log file validation is enabled

Description

CloudTrail log file validation creates a digitally signed digest file containing a hash of each log that CloudTrail writes to S3. These digest files can be used to determine whether a log file was changed, deleted, or unchanged after CloudTrail delivered the log. It is recommended that file validation be enabled on all CloudTrails. Enabling log file validation will provide additional integrity checking of CloudTrail logs.

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: 'aws_cloudtrail[foobar].enable_log_file_validation' is set

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: 'aws_cloudtrail[foobar].enable_log_file_validation' is set

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: 'aws_cloudtrail[foobar].enable_log_file_validation' is set

Cloudfront Without WAF

Results **4**

Severity	LOW
Platform	Terraform
Category	Networking and Firewall

Description

All AWS CloudFront distributions should be integrated with the Web Application Firewall (AWS WAF) service

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:44

Expected: 'web_acl_id' exists

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:14

Expected: 'web_acl_id' exists

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:14

Expected: 'web_acl_id' exists

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:32

Expected: 'web_acl_id' exists

DocDB Logging Is Disabled

Results **4**

Severity LOW
Platform Terraform
Category Observability

Description

DocDB logging should be enabled

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_without_kms_key/main.tf:5

Expected: aws_docdb_cluster.enabled_cloudwatch_logs_exports is defined

test-cases/terraform/aws/logging/docdb_audit_logs_missing/main.tf:1

Expected: aws_docdb_cluster.enabled_cloudwatch_logs_exports is defined

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_at_rest_using_cmk_not_customer_managed/main.tf:9

Expected: aws_docdb_cluster.enabled_cloudwatch_logs_exports is defined

test-cases/terraform/aws/encryption/at-rest/docdb_clusters_non_encrypted/main.tf:5

Expected: aws_docdb_cluster.enabled_cloudwatch_logs_exports is defined

EC2 Instance Using Default Security Group

Results **5**

Severity LOW
Platform Terraform
Category Access Control

Description

EC2 instances should not use default security group(s)

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:67

Expected: aws_instance[ec2].vpc_security_group_ids is not using default security group

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:65

Expected: aws_instance[ec2].vpc_security_group_ids is not using default security group

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:83

Expected: aws_instance[inst1].vpc_security_group_ids is not using default security group

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:109

Expected: aws_instance[inst3].vpc_security_group_ids is not using default security group

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:96

Expected: aws_instance[inst2].vpc_security_group_ids is not using default security group

EC2 Instance Using Default VPC

Results **4**

Severity LOW
Platform Terraform
Category Networking and Firewall

Description

EC2 Instances should not be configured under a default VPC network

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:136

Expected: aws_instance[public_ins].subnet_id is not associated with a default VPC

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:143

Expected: aws_instance[public_ins].subnet_id is not associated with a default VPC

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:151

Expected: aws_instance[public_ins].subnet_id is not associated with a default VPC

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:52

Expected: aws_instance[t2-instance].subnet_id is not associated with a default VPC

ECR Repository Without Policy

Results **4**

Severity LOW
Platform Terraform
Category Best Practices

Description

ECR Repository should have Policies attached to it

test-cases/terraform/aws/best-practices/ecr_make_tags_immutable/main.tf:1

Expected: aws_ecr_repository[foo] has policies attached

test-cases/terraform/aws/best-practices/ecr_use_image_scanning/main.tf:1

Expected: aws_ecr_repository[foo] has policies attached

test-cases/terraform/aws/iam/resource-policies/ecr_not_secure_policy/main.tf:1

Expected: aws_ecr_repository[foo] has policies attached

test-cases/terraform/aws/encryption/at-rest/ecr_repo_not_encrypted/main.tf:1

Expected: aws_ecr_repository[foo] has policies attached

ECS Cluster with Container Insights Disabled

Results **1**

Severity LOW
Platform Terraform
Category Observability

Description

ECS Cluster should enable container insights

test-cases/terraform/aws/best-practices/ecs_cluster_container_insights/main.tf:1

Expected: 'aws_ecs_cluster[foo].setting.name' is set to 'containerInsights' and 'aws_ecs_cluster[foo].setting.value' is set to 'enabled'

EKS cluster logging is not enabled

Results **1**

Severity LOW
Platform Terraform
Category Observability

Description

Amazon EKS control plane logging is not enabled

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:19

Expected: 'enabled_cluster_log_types' is defined and not null

ElastiCache Using Default Port

Results **2**

Severity LOW
Platform Terraform

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Category Networking and Firewall

Description

ElastiCache should not use the default port (an attacker can easily guess the port). For engine set to Redis, the default port is 6379. The Memcached default port is 11211

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:1

Expected: aws_elasticache_cluster.port is defined and not null

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:9

Expected: aws_elasticache_cluster.port is defined and not null

ElastiCache Without VPC

Results **2**

Severity LOW
Platform Terraform
Category Networking and Firewall

Description

ElastiCache should be launched in a Virtual Private Cloud (VPC)

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:1

Expected: 'aws_elasticache_cluster[default].subnet_group_name' is defined and not null'

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:9

Expected: 'aws_elasticache_cluster[disabled].subnet_group_name' is defined and not null'

Function App HTTP2 Disabled

Results **9**

Severity LOW
Platform Terraform
Category Insecure Configurations

Description

Function App should have 'http2_enabled' enabled

test-cases/terraform/azure/iam/func_app_client_cert_optional/main.tf:43

Expected: 'azurerm_function_app[functionapp].site_config' is defined and not null

test-cases/terraform/azure/encryption/in-transit/func_app_ftps_not_required/main.tf:35

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/iam/func_app_authentication/main.tf:42

Expected: 'azurerm_function_app[functionapp].site_config' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_win_java_isnot_latest/main.tf:60

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/best-practices/functionapp_lin_java_isnot_latest/main.tf:51

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/iam/functionapp_not_use_managedidentity/main.tf:35

Expected: 'azurerm_function_app[functionapp].site_config' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_latest_tls/main.tf:43

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is defined and not null

test-cases/terraform/azure/best-practices/func_app_not_using_http2/main.tf:44

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is set to true

test-cases/terraform/azure/best-practices/functionapp_python_isnot_latest/main.tf:51

Expected: 'azurerm_function_app[functionapp].site_config.http2_enabled' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

Global Accelerator Flow Logs Disabled

Results 1

Severity LOW
Platform Terraform
Category Observability

Description

Global Accelerator should have flow logs enabled

test-cases/terraform/aws/logging/globalaccelerator_accelerator_no_flow_logs/main.tf:6

Expected: aws_globalaccelerator_accelerator[{{example}}].flow_logs_enabled is defined and not null

IAM Policies Attached To User

Results 2

Severity LOW
Platform Terraform
Category Best Practices

Description

IAM policies should be attached only to groups or roles

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:29

Expected: 'user' is redundant

test-cases/terraform/aws/iam/iam-entities/iam_user_inline_policy_attach/main.tf:11

Expected: 'user' is redundant

IAM Policy Grants 'AssumeRole' Permission Across All Services

Results 1

Severity LOW
Platform Terraform
Category Access Control

Description

IAM role allows All services or principals to assume it

test-cases/terraform/aws/iam/iam-entities/role_assume_policy_principal_all/main.tf:25

Expected: 'assume_role_policy.Statement.Principal' doesn't contain '*'

Lambda Functions Without X-Ray Tracing

Results 4

Severity LOW
Platform Terraform
Category Observability

Description

AWS Lambda functions should have TracingConfig enabled. For this, property 'tracing_Config.mode' should have the value 'Active'

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:5

Expected: aws_lambda_function[my-lambda].tracing_config is defined and not null

test-cases/terraform/aws/logging/lambda_without_explicit_log_group/main.tf:57

Expected: aws_lambda_function[test_lambda].tracing_config is defined and not null

test-cases/terraform/aws/logging/lambda_without_xray/main.tf:21

Expected: aws_lambda_function[test_lambda].tracing_config is defined and not null

test-cases/terraform/aws/networking/lambda_not_in_vpc/main.tf:21

Expected: aws_lambda_function[test_lambda].tracing_config is defined and not null

Checkmarx

KICS REPORT vv1.5.2

Lambda Permission Misconfigured

Results 1

Severity LOW
Platform Terraform
Category Best Practices

Description

Lambda permission may be misconfigured if the action field is not filled in by 'lambda:InvokeFunction'

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:35

Expected: aws_lambda_permission[name].action is 'lambda:InvokeFunction'%!(EXTRA string=all)

Open Access To Resources Through API

Results 5

Severity LOW
Platform Terraform
Category Insecure Configurations

Description

Open access to back-end resources through API

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:26

Expected: 'authorization' is not equal 'NONE'

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:26

Expected: 'authorization' is not equal 'NONE'

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:54

Expected: 'authorization' is not equal 'NONE'

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:26

Expected: 'authorization' is not equal 'NONE'

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:26

Expected: 'authorization' is not equal 'NONE'

PostgreSQL Server Infrastructure Encryption Disabled

Results 4

Severity LOW
Platform Terraform
Category Encryption

Description

PostgreSQL Server Infrastructure Encryption should be enabled

test-cases/terraform/azure/logging/postgresql_log_connections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server[example].infrastructure_encryption_enabled' is defined and set to true

test-cases/terraform/azure/encryption/in-transit/postgresql_not_forcing_ssl/main.tf:15

Expected: 'azurerm_postgresql_server[example].infrastructure_encryption_enabled' is defined and set to true

test-cases/terraform/azure/logging/postgresql_log_disconnections_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server[example].infrastructure_encryption_enabled' is defined and set to true

test-cases/terraform/azure/logging/postgresql_logcheckpoints_not_enabled/main.tf:15

Expected: 'azurerm_postgresql_server[example].infrastructure_encryption_enabled' is defined and set to true

Redshift Using Default Port

Results 4

Severity LOW
Platform Terraform

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Category Networking and Firewall

Description

Redshift should not use the default port (5439) because an attacker can easily guess the port

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster.port is defined and not null

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster.port is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:103

Expected: aws_redshift_cluster.port is defined and not null

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Expected: aws_redshift_cluster.port is defined and not null

S3 Bucket Logging Disabled

Results **18**

Severity LOW
Platform Terraform
Category Observability

Description

S3 bucket without logging

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: 'logging' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:1

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:32

Expected: 'logging' is defined and not null

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:1

Expected: 'logging' is defined and not null

test-cases/terraform/aws/logging/s3_access_logging_disabled/main.tf:1

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_non_encrypted/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:33

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:5

Expected: 'logging' is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: 'logging' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: 'logging' is defined and not null

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:1

Expected: 'logging' is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: 'logging' is defined and not null

S3 Bucket Public ACL Overridden By Public Access Block

Results **2**

Severity	LOW
Platform	Terraform
Category	Access Control
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.1.5
Title	Ensure that S3 Buckets are configured with 'Block public access (bucket settings)'

Description

Amazon S3 provides Block public access (bucket settings) and Block public access (account settings) to help you manage public access to Amazon S3 resources. By default, S3 buckets and objects are created with public access disabled. However, an IAM principal with sufficient S3 permissions can enable public access at the bucket and/or object level. While enabled, Block public access (bucket settings) prevents an individual bucket, and its contained objects, from becoming publicly accessible. Similarly, Block public access (account settings) prevents all buckets, and contained objects, from becoming publicly accessible across the entire account. Amazon S3 Block public access (bucket settings) prevents the accidental or malicious public exposure of data contained within the respective bucket(s). Amazon S3 Block public access (account settings) prevents the accidental or malicious public exposure of data contained within all buckets of the respective AWS account. Whether blocking public access to all or some buckets is an organizational decision that should be based on data sensitivity, least privilege, and use case.

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:7

Expected: S3 Bucket public ACL is not overridden by S3 bucket Public Access Block

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:7

Expected: S3 Bucket public ACL is not overridden by S3 bucket Public Access Block

Shield Advanced Not In Use

Results **10**

Severity	LOW
Platform	Terraform
Category	Networking and Firewall

Description

AWS Shield Advanced should be used for Amazon Route 53 hosted zone, AWS Global Accelerator accelerator, Elastic IP Address, Elastic Load Balancing, and Amazon CloudFront Distribution to protect these resources against robust DDoS attacks

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:56

Expected: aws_eip has shield advanced associated

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: aws_lb has shield advanced associated

test-cases/terraform/aws/logging/globalaccelerator_accelerator_no_flow_logs/main.tf:1

Expected: aws_globalaccelerator_accelerator has shield advanced associated

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:32

Expected: aws_cloudfront_distribution has shield advanced associated

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:44

Expected: aws_cloudfront_distribution has shield advanced associated

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:49

Expected: aws_lb has shield advanced associated

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:60

Expected: aws_lb has shield advanced associated

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:39

Expected: aws_lb has shield advanced associated

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:14

Expected: aws_cloudfront_distribution has shield advanced associated

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:14

Expected: aws_cloudfront_distribution has shield advanced associated

App Service Authentication Disabled

Results **9**

Severity	INFO
Platform	Terraform
Category	Access Control

Description

Azure App Service authentication settings should be enabled

test-cases/terraform/azure/encryption/in-transit/app_service_use_most_recent_supported_tls/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/encryption/in-transit/app_service_ftps_unused/main.tf:36

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/best-practices/webapp_http2_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/best-practices/webapp_lin_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/best-practices/webapp_php_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/best-practices/webapp_win_java_isnot_latest/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/iam/webapp_client_cert_not_enabled/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/iam/app_service_authentication_missing/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

test-cases/terraform/azure/iam/webapp_not_use_managedidentity/main.tf:28

Expected: 'azurerm_app_service[webapp].auth_settings' is defined

DynamoDB Table Point In Time Recovery Disabled

Results **4**

Checkmarx

KICS REPORT vv1.5.2

Severity INFO
Platform Terraform
Category Best Practices

Description

It's considered a best practice to have point in time recovery enabled for DynamoDB Table

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:143

Expected: aws_dynamodb_table.point_in_time_recovery.enabled is enabled

test-cases/terraform/aws/best-practices/dynamodb_without_recovery_enabled/main.tf:1

Expected: aws_dynamodb_table.point_in_time_recovery.enabled is enabled

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:90

Expected: aws_dynamodb_table.point_in_time_recovery.enabled is enabled

test-cases/terraform/aws/encryption/at-rest/dynamodb_not_encrypted/main.tf:1

Expected: aws_dynamodb_table.point_in_time_recovery.enabled is enabled

EC2 Instance Monitoring Disabled

Results **21**

Severity INFO
Platform Terraform
Category Observability

Description

EC2 Instance should have detailed monitoring enabled. With detailed monitoring enabled data is available in 1-minute periods

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:136

Expected: 'monitoring' is defined and not null%!(EXTRA string=test)

test-cases/terraform/aws/logging/ec2_without_monitoring/main.tf:17

Expected: 'monitoring' is defined and not null%!(EXTRA string=web)

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: 'monitoring' is defined and not null%!(EXTRA string=t2-instance)

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:82

Expected: 'monitoring' is defined and not null%!(EXTRA string=inst1)

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:80

Expected: 'monitoring' is defined and not null%!(EXTRA string=example_with_copied_ami)

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:146

Expected: 'monitoring' is defined and not null%!(EXTRA string=public_ins)

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:45

Expected: 'monitoring' is defined and not null%!(EXTRA string=example_with_new_ami)

test-cases/terraform/aws/best-practices/ec2_ebs_not_optimized/main.tf:17

Expected: 'monitoring' is defined and not null%!(EXTRA string=web)

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:131

Expected: 'monitoring' is defined and not null%!(EXTRA string=public_ins)

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:31

Expected: 'monitoring' is defined and not null%!(EXTRA string=ec2)

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:95

Expected: 'monitoring' is defined and not null%!(EXTRA string=inst2)

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:108

Expected: 'monitoring' is defined and not null%!(EXTRA string=inst3)

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:138

Expected: 'monitoring' is defined and not null%!(EXTRA string=public_ins)

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:98

Expected: 'monitoring' is defined and not null%!(EXTRA string=pub_ins)

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:61

Expected: 'monitoring' is defined and not null%!(EXTRA string=ec2)

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:87

Expected: 'monitoring' is defined and not null%!(EXTRA string=test-ec2-instance)

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:63

Expected: 'monitoring' is defined and not null%!(EXTRA string=ec2)

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:98

Expected: 'monitoring' is defined and not null%!(EXTRA string=public-ubuntu-from-data)

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:93

Expected: 'monitoring' is defined and not null%!(EXTRA string=example_with_ami_from_instance)

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:106

Expected: 'monitoring' is defined and not null%!(EXTRA string=priv_ins)

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:83

Expected: 'monitoring' is defined and not null%!(EXTRA string=test)

EC2 Not EBS Optimized

Results **21**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

It's considered a best practice for an EC2 instance to use an EBS optimized instance. This provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance

test-cases/terraform/aws/logging/ec2_without_monitoring/main.tf:17

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:63

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:80

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:146

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:45

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:138

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:98

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:95

Expected: 'ebs_optimized' is set to true

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:82

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:31

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:93

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/ec2_ebs_not_optimized/main.tf:17

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:98

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:136

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:83

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:106

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:87

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:61

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:108

Expected: 'ebs_optimized' is set to true

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:131

Expected: 'ebs_optimized' is set to true

ELB Access Logging Disabled

Results **1**

Severity	INFO
Platform	Terraform
Category	Observability

Description

ELB should have logging enabled to help on error investigation

test-cases/terraform/aws/logging/elb_without_access_logs/main.tf:1

Expected: 'aws_elb[{{test}}].access_logs' is defined and not null

Name Is Not Snake Case

Results **63**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All names should follow snake case pattern.

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:28

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Checkmarx

KICS REPORT vv1.5.2

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:98

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/best-practices/dynamodb_without_recovery_enabled/main.tf:1

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:13

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:112

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:18

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:37

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:103

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/at-rest/codbuild_using_aws_key/main.tf:29

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:27

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:12

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/at-rest/dax_cluster_not_encrypted/main.tf:25

Expected: All names should be on snake case pattern

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:43

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:80

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:94

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:28

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:32

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:87

Expected: All names should be on snake case pattern

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:24

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/role_assume_policy_principal_all/main.tf:22

Expected: All names should be on snake case pattern

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:53

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/at-rest/cloudwatch_groups_not_encrypted/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:21

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:56

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:13

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:45

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:61

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:47

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:32

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:22

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:66

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/at-rest/dynamodb_not_encrypted/main.tf:1

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:98

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:9

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:30

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:90

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/role_assume_policy_principal_all/main.tf:4

Expected: All names should be on snake case pattern

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:18

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:35

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:38

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:10

Checkmarx

KICS REPORT vv1.5.2

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:27

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:44

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:22

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:143

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:25

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:45

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:20

Expected: All names should be on snake case pattern

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: All names should be on snake case pattern

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:35

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:50

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: All names should be on snake case pattern

test-cases/terraform/azure/networking/public_access_sql_db/main.tf:16

Expected: All names should be on snake case pattern

test-cases/terraform/aws/iam/iam-entities/iam_user_inline_policy_attach/main.tf:5

Expected: All names should be on snake case pattern

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:33

Expected: All names should be on snake case pattern

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:17

Expected: All names should be on snake case pattern

Neptune Logging Is Disabled

Results **3**

Severity	INFO
Platform	Terraform
Category	Observability

Description

Neptune logging should be enabled

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:66

Expected: aws_neptune_cluster.enable_cloudwatch_logs_exports is defined

test-cases/terraform/aws/logging/neptune_cluster_no_logging/main.tf:1

Expected: aws_neptune_cluster.enable_cloudwatch_logs_exports is defined

test-cases/terraform/aws/encryption/at-rest/neptune_cluster_no_encryption/main.tf:1

Expected: aws_neptune_cluster.enable_cloudwatch_logs_exports is defined

Checkmarx

KICS REPORT vv1.5.2

RDS Without Logging

Results 4

Severity INFO
Platform Terraform
Category Observability

Description

RDS does not have any kind of logger

test-cases/terraform/aws/logging/rds_without_logging/main.tf:1

Expected: 'enabled_cloudwatch_logs_exports' is defined

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:1

Expected: 'enabled_cloudwatch_logs_exports' is defined

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:113

Expected: 'enabled_cloudwatch_logs_exports' is defined

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:60

Expected: 'enabled_cloudwatch_logs_exports' is defined

Resource Not Using Tags

Results 266

Severity INFO
Platform Terraform
Category Best Practices

Description

AWS services resource tags are an essential part of managing components

test-cases/terraform/aws/logging/neptune_cluster_no_logging/main.tf:1

Expected: aws_neptune_cluster[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:97

Expected: aws_redshift_subnet_group[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/human_users_defined/main.tf:5

Expected: aws_iam_user[{{iam_user_1}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:75

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:8

Expected: aws_vpc[{{main}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:42

Expected: aws_route_table[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/dax_cluster_not_encrypted/main.tf:6

Expected: aws_iam_role[{{dax}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:107

Expected: aws_elasticsearch_domain[{{test}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:18

Expected: aws_s3_bucket[{{foo}}].tags is defined and not null

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:6

Expected: aws_iam_role[{{eksrole}}].tags is defined and not null

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:18

Expected: aws_subnet[{{default-subnet}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:98

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_instance[{{pub_ins}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:17

Expected: aws_subnet[{{private-subnet}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/ecr_make_tags_immutable/main.tf:1

Expected: aws_ecr_repository[{{foo}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:28

Expected: aws_security_group[{{allow_tls}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_at_rest_using_cmk_not_customer_managed/main.tf:9

Expected: aws_docdb_cluster[{{test2}}].tags is defined and not null

test-cases/terraform/aws/logging/ec2_without_monitoring/main.tf:21

Expected: aws_instance[{{web}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:26

Expected: aws_subnet[{{subnet}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:10

Expected: aws_s3_bucket[{{cdn-content}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/docdb_clusters_non_encrypted/main.tf:5

Expected: aws_docdb_cluster[{{docdb}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:28

Expected: aws_route_table[{{public-rtb}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:34

Expected: aws_subnet[{{subnet1}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:79

Expected: aws_route_table[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:18

Expected: aws_s3_bucket[{{foo}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:38

Expected: aws_glue_crawler[{{cloudrail_table_crawler}}].tags is defined and not null

test-cases/terraform/aws/networking/lambda_not_in_vpc/main.tf:1

Expected: aws_iam_role[{{iam_for_lambda}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:69

Expected: aws_subnet[{{nondefault_2}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:82

Expected: aws_instance[{{inst1}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/rds_cluster_encrypt_at_rest_disabled/main.tf:5

Expected: aws_rds_cluster[{{default}}].tags is defined and not null

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:25

Expected: aws_lb[{{default}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:98

Expected: aws_security_group[{{allow-public-outbound-sg}}].tags is defined and not null

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:5

Expected: aws_api_gateway_rest_api[{{api_gw}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:10

Expected: aws_vpc[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/passrole_and_lambda_permissions_cause_priv_escalation/main.tf:5

Expected: aws_iam_role[{{role}}].tags is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:97

Expected: aws_db_subnet_group[{{db}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:45

Expected: aws_subnet[{{subnet2_2}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:75

Expected: aws_ami_copy[{{example}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:36

Expected: aws_instance[{{ec2}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:32

Expected: aws_directory_service_directory[{{test}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:143

Expected: aws_dynamodb_table[{{basic-dynamodb-table}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:33

Expected: aws_security_group[{{default}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/sns_topic_encrypted_at_rest_with_aws_managed_key_by_key_arn/main.tf:9

Expected: aws_sns_topic[{{test}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:44

Expected: aws_api_gateway_stage[{{api_gw_stage}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/secretsmanager_secrets_encrypted_at_rest_with_aws_managed_key_by_key_arn/main.tf:9

Expected: aws_secretsmanager_secret[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:114

Expected: aws_security_group[{{publicly_accessible_sg}}].tags is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:3

Expected: aws_cloudtrail[{{foobar}}].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_explicit_log_group/main.tf:9

Expected: aws_iam_role[{{iam_for_lambda}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:35

Expected: aws_security_group[{{default}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:5

Expected: aws_s3_bucket[{{cloudrail}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/role_assume_policy_principal_all/main.tf:22

Expected: aws_iam_role[{{over-privilege-role2}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:53

Expected: aws_security_group[{{allow-public-outbound-sg}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:103

Expected: aws_sqs_queue[{{test-queue}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:9

Expected: aws_vpc[{{external}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:1

Expected: aws_elasticache_cluster[{{default}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:5

Expected: aws_lambda_function[{{my-lambda}}].tags is defined and not null

test-cases/terraform/aws/best-practices/kms_uses_rotation/main.tf:1

Expected: aws_kms_key[{{a}}].tags is defined and not null

test-cases/terraform/aws/logging/globalaccelerator_accelerator_no_flow_logs/main.tf:1

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_globalaccelerator_accelerator[{{example}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:27

Expected: aws_subnet[{{subnet2}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:10

Expected: aws_vpc[{{vpc}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:48

Expected: aws_network_acl[{{allow-public-outbound-nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:92

Expected: aws_security_group[{{esdomain}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:71

Expected: aws_iam_instance_profile[{{test_profile}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:31

Expected: aws_network_acl[{{ec2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:50

Expected: aws_dms_replication_subnet_group[{{test}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:42

Expected: aws_subnet[{{private-subnet}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:50

Expected: aws_iam_role[{{test_role}}].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_explicit_log_group/main.tf:29

Expected: aws_iam_policy[{{lambda_logging}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:60

Expected: aws_db_instance[{{test}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:33

Expected: aws_s3_bucket[{{cloudrail}}].tags is defined and not null

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:49

Expected: aws_instance[{{t2-instance}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:10

Expected: aws_vpc[{{vpc}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:5

Expected: aws_vpc[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_distribution_not_encrypted/main.tf:44

Expected: aws_cloudfront_distribution[{{s3_distribution}}].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_explicit_log_group/main.tf:57

Expected: aws_lambda_function[{{test_lambda}}].tags is defined and not null

test-cases/terraform/aws/best-practices/cloudfront_not_using_waf/main.tf:5

Expected: aws_s3_bucket[{{b}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:9

Expected: aws_s3_bucket[{{logging}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:26

Expected: aws_vpc[{{vpc1}}].tags is defined and not null

test-cases/terraform/aws/best-practices/ecr_use_image_scanning/main.tf:1

Expected: aws_ecr_repository[{{foo}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:63

Expected: aws_default_security_group[{{dsg}}].tags is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/hcl_language_complexity/using_for_each/main.tf:4

Expected: aws_iam_user[{{example}}].tags is defined and not null

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:10

Expected: aws_vpc[{{vpc}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:18

Expected: aws_security_group[{{free}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/rest_api_cache_non_encrypted/main.tf:5

Expected: aws_api_gateway_rest_api[{{api_gw}}].tags is defined and not null

test-cases/terraform/aws/best-practices/tag_all_items/plan.json:55

Expected: aws_sqs_queue[{{cloudrail}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/iam/iam-entities/human_users_defined/main.tf:15

Expected: aws_iam_user[{{iam_user_2}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:47

Expected: aws_workspaces_directory[{{test}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:5

Expected: aws_iam_user[{{user-1}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:32

Expected: aws_internet_gateway[{{igw1}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:87

Expected: aws_instance[{{test-ec2-instance}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:22

Expected: aws_subnet[{{public-subnet}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:88

Expected: aws_ami_from_instance[{{example}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/neptune_cluster_no_encryption/main.tf:1

Expected: aws_neptune_cluster[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:36

Expected: aws_network_acl[{{ec2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:84

Expected: aws_route_table[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:92

Expected: aws_vpc_peering_connection[{{this}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/policy-too-broad/main.tf:5

Expected: aws_iam_role[{{role}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:103

Expected: aws_security_group[{{db}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:74

Expected: aws_subnet[{{nondefault_2}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/elasticache_replication_group_not_encrypted_at_rest/main.tf:1

Expected: aws_elasticache_replication_group[{{example}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:19

Expected: aws_ebs_volume[{{example}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/deploy_redshift_in_ec2_classic_mode/main.tf:5

Expected: aws_redshift_cluster[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:121

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_security_group[{{publicly_accessible_sg}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/public_and_private_ec2_same_role/main.tf:106

Expected: aws_instance[{{priv_ins}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:56

Expected: aws_lb_target_group[{{test}}].tags is defined and not null

test-cases/terraform/aws/logging/cloudtrail_file_log_validation_disabled/main.tf:11

Expected: aws_cloudtrail[{{foobar}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:93

Expected: aws_network_acl[{{allow-public-outbound-nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:63

Expected: aws_subnet[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:67

Expected: aws_dms_replication_instance[{{test}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:25

Expected: aws_route_table[{{private-rtb}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:107

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:47

Expected: aws_workspaces_directory[{{test}}].tags is defined and not null

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:5

Expected: aws_api_gateway_rest_api[{{api_gw}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/dax_cluster_not_encrypted/main.tf:25

Expected: aws_dax_cluster[{{cloudrail-test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:113

Expected: aws_db_instance[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:84

Expected: aws_route_table[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:5

Expected: aws_api_gateway_rest_api[{{api_gw}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:51

Expected: aws_nat_gateway[{{private-subnet-nat-gw}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:27

Expected: aws_ebs_snapshot[{{example_snapshot}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:50

Expected: aws_security_group[{{public-internet-sg}}].tags is defined and not null

test-cases/terraform/aws/best-practices/alb_drop_http_headers/main.tf:39

Expected: aws_lb[{{disabled}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:40

Expected: aws_subnet[{{subnet}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:76

Expected: aws_neptune_cluster_instance[{{neptune_instance}}].tags is defined and not null

test-cases/terraform/aws/logging/api_gateway_no_xray/main.tf:44

Expected: aws_api_gateway_stage[{{api_gw_stage}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/secretsmanager_secrets_encrypted_at_rest_with_aws_managed_key_by_default/main.tf:5

Expected: aws_secretsmanager_secret[{{test}}].tags is defined and not null

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/encryption/at-rest/cloudwatch_groups_not_encrypted/main.tf:5

Expected: aws_cloudwatch_log_group[{{cloudrail-test}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:61

Expected: aws_iam_role[{{workspaces_default}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/elasticsearch_encrypt_node_to_node_disabled/main.tf:5

Expected: aws_elasticsearch_domain[{{example}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:29

Expected: aws_route_table[{{rt}}].tags is defined and not null

test-cases/terraform/aws/logging/redshift_without_logging/main.tf:1

Expected: aws_redshift_cluster[{{default}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/sagemaker_not_encrypted/main.tf:28

Expected: aws_sagemaker_notebook_instance[{{ni}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:32

Expected: aws_s3_bucket[{{cloudrail_anthena_bucket_2}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:162

Expected: aws_route_table[{{subnet2_1}}].tags is defined and not null

test-cases/terraform/aws/networking/lambda_not_in_vpc/main.tf:21

Expected: aws_lambda_function[{{test_lambda}}].tags is defined and not null

test-cases/terraform/hcl_language_complexity/using_count_and_ternary_expr/main.tf:22

Expected: aws_iam_user[{{jill}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:80

Expected: aws_instance[{{example_with_copied_ami}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/codbuild_using_aws_key/main.tf:10

Expected: aws_iam_role[{{codebuild}}].tags is defined and not null

test-cases/terraform/aws/best-practices/tag_all_items/main.tf:7

Expected: aws_sns_topic[{{cloudrail_1}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:129

Expected: aws_security_group[{{publicly_accessible_sg}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:20

Expected: aws_subnet[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/athena_not_encrypted/main.tf:1

Expected: aws_s3_bucket[{{hoge}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:5

Expected: aws_api_gateway_rest_api[{{api_gw}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:5

Expected: aws_vpc[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:54

Expected: aws_lb_target_group[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:59

Expected: aws_db_subnet_group[{{free}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:9

Expected: aws_security_group[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:38

Expected: aws_subnet[{{subnet}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:103

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_redshift_cluster[{{test}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/cloudtrail_not_encrypted/main.tf:11

Expected: aws_cloudtrail[{{foobar}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:45

Expected: aws_athena_workgroup[{{cloudrail_wg_2}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:94

Expected: aws_vpc_endpoint[{{sqs-vpc-endpoint}}].tags is defined and not null

test-cases/terraform/aws/logging/cloudfront_distribution_without_logging/main.tf:5

Expected: aws_s3_bucket[{{b}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:80

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:115

Expected: aws_internet_gateway[{{internet-gateway}}].tags has tags defined other than 'Name'

test-cases/terraform/hcl_language_complexity/using_module_multi/mymodule/user.tf:13

Expected: aws_iam_user[{{user}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_non_encrypted/main.tf:5

Expected: aws_s3_bucket[{{cloudrail}}].tags is defined and not null

test-cases/terraform/hcl_language_complexity/using_locals/main.tf:5

Expected: aws_iam_user[{{example}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/docdb_cluster_encrypted_without_kms_key/main.tf:5

Expected: aws_docdb_cluster[{{test1}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:12

Expected: aws_vpc[{{main}}].tags is defined and not null

test-cases/terraform/aws/best-practices/cloudtrail_enabled_on_multi_region/main.tf:10

Expected: aws_s3_bucket[{{foo}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/glacier_vault_not_secure_policy/main.tf:9

Expected: aws_glacier_vault[{{not_secure_archive}}].tags is defined and not null

test-cases/terraform/aws/best-practices/tag_all_items/main.tf:14

Expected: aws_sqs_queue[{{cloudrail}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:3

Expected: aws_vpc[{{example}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:138

Expected: aws_instance[{{public_ins}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:53

Expected: aws_subnet[{{free_2}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:32

Expected: aws_db_subnet_group[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/role_assume_policy_principal_all/main.tf:4

Expected: aws_iam_role[{{over-privilege-role1}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/rest_api_not_secure_policy/main.tf:72

Expected: aws_api_gateway_stage[{{api_gw_stage}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:47

Expected: aws_subnet[{{free_1}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/iam_user_inline_policy_attach/main.tf:5

Expected: aws_iam_user[{{user-1}}].tags is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:10

Expected: aws_vpc[{{nondefault}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:61

Expected: aws_instance[{{ec2}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/codbuild_using_aws_key/main.tf:29

Expected: aws_codebuild_project[{{project-cloudrail-test}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/kms_key_not_secure_policy/main.tf:5

Expected: aws_kms_key[{{not_secure_policy}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:76

Expected: aws_workspaces_workspace[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:146

Expected: aws_instance[{{public_ins}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/elasticache_replication_group_not_encrypted_in_transit/main.tf:5

Expected: aws_elasticache_replication_group[{{example}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned/main.tf:5

Expected: aws_s3_bucket[{{public-bucket}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/s3_bucket_object_non_encrypted/main.tf:18

Expected: aws_s3_bucket_object[{{object}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/glue_data_catalog_not_secure_policy/main.tf:14

Expected: aws_iam_role[{{cloudrail_glue_iam}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:38

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/redshift_not_encrypted/main.tf:5

Expected: aws_redshift_cluster[{{default}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:17

Expected: aws_subnet[{{subnet1}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:40

Expected: aws_subnet[{{subnet2_1}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:44

Expected: aws_subnet[{{subnet2}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:56

Expected: aws_eip[{{allocate-ip-to-nat-gw}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:90

Expected: aws_dynamodb_table[{{basic-dynamodb-table}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:5

Expected: aws_vpc[{{vpc1}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/ecr_not_secure_policy/main.tf:1

Expected: aws_ecr_repository[{{foo}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:136

Expected: aws_instance[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:14

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:66

Expected: aws_neptune_cluster[{{encrypted_neptune_cluster}}].tags is defined and not null

test-cases/terraform/aws/best-practices/elasticache_automatic_backup/main.tf:9

https://kics.io

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_elasticache_cluster[{{disabled}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:12

Expected: aws_iam_role[{{dms-access-for-endpoint}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:30

Expected: aws_subnet[{{subnet1_2}}].tags is defined and not null

test-cases/terraform/aws/best-practices/tag_all_items/plan.json:32

Expected: aws_sns_topic[{{cloudrail_1}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:93

Expected: aws_instance[{{example_with_ami_from_instance}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_user_volume_not_encrypted_at_rest/main.tf:32

Expected: aws_directory_service_directory[{{test}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:5

Expected: aws_vpc[{{main}}].tags is defined and not null

test-cases/terraform/aws/best-practices/rds_retention_period_set/main.tf:1

Expected: aws_rds_cluster[{{default}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:40

Expected: aws_route_table[{{public-rtb}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:76

Expected: aws_workspaces_workspace[{{test}}].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_xray/main.tf:1

Expected: aws_iam_role[{{iam_for_lambda}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:36

Expected: aws_network_acl[{{ec2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:108

Expected: aws_instance[{{inst3}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:103

Expected: aws_vpc_peering_connection_accepter[{{peer_accepter}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:75

Expected: aws_route_table[{{private-rtb}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:68

Expected: aws_subnet[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:68

Expected: aws_subnet[{{nondefault_1}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_authenticated_users_canned/main.tf:5

Expected: aws_s3_bucket[{{public-bucket}}].tags is defined and not null

test-cases/terraform/aws/logging/elb_without_access_logs/main.tf:1

Expected: aws_elb[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:26

Expected: aws_subnet[{{nondefault_2}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/policy_missing_principal/main.tf:5

Expected: aws_kms_key[{{secure_policy}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/lambda_not_secure_policy/main.tf:13

Expected: aws_iam_role[{{lambda-role}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:102

Expected: aws_instance[{{public-ubuntu-from-data}}].tags has tags defined other than 'Name'

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:5

Expected: aws_s3_bucket[{{cloudrail_anthena_bucket}}].tags is defined and not null

test-cases/terraform/aws/logging/rds_without_logging/main.tf:1

Expected: aws_db_instance[{{default}}].tags is defined and not null

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:19

Expected: aws_eks_cluster[{{test}}].tags is defined and not null

test-cases/terraform/hcl_language_complexity/using_count_and_ternary_expr/main.tf:10

Expected: aws_iam_user[{{jack}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/workspace_root_volume_not_encrypted_at_rest/main.tf:61

Expected: aws_iam_role[{{workspaces_default}}].tags is defined and not null

test-cases/terraform/aws/best-practices/config_aggregator_all_regions/main.tf:1

Expected: aws_config_configuration_aggregator[{{organization}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/ecr_repo_not_encrypted/main.tf:1

Expected: aws_ecr_repository[{{foo}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:49

Expected: aws_lb[{{test}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:131

Expected: aws_instance[{{public_ins}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:74

Expected: aws_subnet[{{nondefault_2}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:25

Expected: aws_subnet[{{subnet1_1}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:60

Expected: aws_lb[{{alb_test}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:45

Expected: aws_instance[{{example_with_new_ami}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/alb_use_http/main.tf:95

Expected: aws_instance[{{inst2}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:63

Expected: aws_network_acl[{{redshift_eni2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:32

Expected: aws_iam_role[{{dms-vpc-role}}].tags is defined and not null

test-cases/terraform/aws/encryption/at-rest/sqs_queue_not_encrypted/main.tf:5

Expected: aws_sqs_queue[{{cloudrail}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/elasticsearch_domain_not_secure_policy/main.tf:5

Expected: aws_elasticsearch_domain[{{es-not-secure-policy}}].tags is defined and not null

test-cases/terraform/aws/best-practices/ec2_ebs_not_optimized/main.tf:21

Expected: aws_instance[{{web}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/at-rest/workgroups_non_encrypted/main.tf:18

Expected: aws_athena_workgroup[{{cloudrail_wg}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:58

Expected: aws_network_acl[{{redshift_eni2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/iam/resource-policies/glacier_vault_not_secure_policy/main.tf:5

Expected: aws_sns_topic[{{aws_sns_topic}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/cloudwatch_log_destination_insecure_policy/main.tf:49

Checkmarx

KICS REPORT vv1.5.2

Expected: aws_kinesis_stream[{{kinesis_for_cloudwatch}}].tags is defined and not null

test-cases/terraform/aws/networking/default_sg_in_new_vpc/main.tf:17

Expected: aws_vpc[{{vpc}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/logging/docdb_audit_logs_missing/main.tf:1

Expected: aws_docdb_cluster[{{docdb}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-authentication/rest_api_without_authorization/main.tf:44

Expected: aws_api_gateway_stage[{{api_gw_stage}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:83

Expected: aws_instance[{{test}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/secrets_manager_not_secure_policy/main.tf:5

Expected: aws_secretsmanager_secret[{{not_secure_policy}}].tags is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:63

Expected: aws_instance[{{ec2}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_acl_public_all_users_canned_with_overriding_access_block/main.tf:5

Expected: aws_s3_bucket[{{public-bucket}}].tags is defined and not null

test-cases/terraform/aws/logging/rest_api_no_access_logging/main.tf:44

Expected: aws_api_gateway_stage[{{api_gw_stage}}].tags is defined and not null

test-cases/terraform/aws/best-practices/using_public_amis/main.tf:32

Expected: aws_ami[{{example}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/s3_bucket_policy_public_to_all_authenticated_users/main.tf:5

Expected: aws_s3_bucket[{{public-bucket}}].tags is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_dms/main.tf:22

Expected: aws_iam_role[{{dms-cloudwatch-logs-role}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/load_balancer_listener_http/main.tf:36

Expected: aws_route_table[{{rt1}}].tags is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:63

Expected: aws_network_acl[{{redshift_eni2_nacl}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:15

Expected: aws_subnet[{{public-subnet}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:80

Expected: aws_internet_gateway[{{igw}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/efs_not_secure_policy/main.tf:8

Expected: aws_efs_file_system[{{not_secure}}].tags has tags defined other than 'Name'

test-cases/terraform/aws/best-practices/ecs_cluster_container_insights/main.tf:1

Expected: aws_ecs_cluster[{{foo}}].tags is defined and not null

test-cases/terraform/aws/logging/eks_logging_disabled/main.tf:14

Expected: aws_subnet[{{subnet1}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/ecs_task_definition_not_encrypted_in_transit/main.tf:9

Expected: aws_ecs_task_definition[{{service}}].tags is defined and not null

test-cases/terraform/aws/iam/iam-entities/iam_user_managed_policy_direct_attachment/main.tf:9

Expected: aws_iam_policy[{{managed-policy}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-policies/cloudwatch_log_destination_insecure_policy/main.tf:29

Expected: aws_iam_role[{{iam_for_cloudwatch}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/cloudfront_protocol_version_is_low/main.tf:18

Expected: aws_s3_bucket[{{dist}}].tags has tags defined other than 'Name'

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:20

Expected: aws_vpc[{{vpc1}}].tags is defined and not null

test-cases/terraform/aws/iam/resource-authentication/rds_without_authentication/main.tf:1

Expected: aws_db_instance[{{default}}].tags is defined and not null

test-cases/terraform/aws/logging/lambda_without_xray/main.tf:21

Expected: aws_lambda_function[{{test_lambda}}].tags is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:30

Expected: aws_vpc_endpoint[{{dynamodb-vpce-gw}}].tags is defined and not null

test-cases/terraform/aws/encryption/in-transit/ecs_task_definition_not_encrypted_in_transit/main.tf:5

Expected: aws_efs_file_system[{{test}}].tags is defined and not null

test-cases/terraform/aws/best-practices/deploy_ec2_to_default_vpc/main.tf:24

Expected: aws_route_table[{{default-route-table}}].tags is defined and not null

test-cases/terraform/aws/networking/over_exposed_vpc_peering/main.tf:35

Expected: aws_vpc[{{vpc2}}].tags is defined and not null

SQL Server Alert Email Disabled

Results **1**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

SQL Server alert email should be enabled

test-cases/terraform/azure/best-practices/sql_vulnerability_email_not_set/main.tf:38

Expected: 'azurerm_mssql_server_security_alert_policy[example].email_account_admins' is defined

Security Group Not Used

Results **2**

Severity	INFO
Platform	Terraform
Category	Access Control

Description

Security group must be used or not declared

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:92

Expected: 'aws_security_group[esdomain]' is used

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:7

Expected: 'aws_security_group[allow_tls]' is used

Security Group Rules Without Description

Results **17**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

It's considered a best practice for all rules in AWS Security Group to have a description

test-cases/terraform/aws/networking/vpc-endpoints/dynamodb-vpce-exist-without-routeassociation/main.tf:58

Expected: aws_security_group[{{allow-public-outbound-sg}}].egress description is defined and not null

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:21

Expected: aws_security_group[{{free}}].ingress description is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:62

Expected: aws_security_group[{{public-internet-sg}}].ingress description is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:19

Expected: aws_security_group[{{default}}].ingress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:94

Expected: aws_security_group[{{esdomain}}].ingress description is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_unused/main.tf:20

Expected: aws_security_group[{{allow_tls}}].egress description is defined and not null

test-cases/terraform/aws/encryption/in-transit/vpc_has_only_dynamodb_vpce_gw_connection/main.tf:103

Expected: aws_security_group[{{allow-public-outbound-sg}}].egress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:116

Expected: aws_security_group[{{publicly_accessible_sg}}].ingress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:137

Expected: aws_security_group[{{publicly_accessible_sg}}].egress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:129

Expected: aws_security_group[{{publicly_accessible_sg}}].egress description is defined and not null

test-cases/terraform/aws/networking/vpc-endpoints/sqs-vpc-endpoint-without-dns-resolution/main.tf:55

Expected: aws_security_group[{{public-internet-sg}}].egress description is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:26

Expected: aws_security_group[{{default}}].egress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:131

Expected: aws_security_group[{{publicly_accessible_sg}}].ingress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:105

Expected: aws_security_group[{{db}}].ingress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:122

Expected: aws_security_group[{{publicly_accessible_sg}}].egress description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:123

Expected: aws_security_group[{{publicly_accessible_sg}}].ingress description is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:12

Expected: aws_security_group[{{nondefault}}].ingress description is defined and not null

Security Group Without Description

Results **9**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

It's considered a best practice for AWS Security Group to have a description

test-cases/terraform/aws/networking/publicly_accessible_neptune_db/main.tf:18

Expected: aws_security_group[{{free}}] description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:129

Expected: aws_security_group[{{publicly_accessible_sg}}] description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:121

Expected: aws_security_group[{{publicly_accessible_sg}}] description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_domain/main.tf:92

Expected: aws_security_group[{{esdomain}}] description is defined and not null

Checkmarx

KICS REPORT vv1.5.2

test-cases/terraform/aws/networking/public_ec2_points_to_private_rds/main.tf:103

Expected: aws_security_group[{{db}}] description is defined and not null

test-cases/terraform/aws/networking/rds-vpc-controlled-public/main.tf:9

Expected: aws_security_group[{{nondefault}}] description is defined and not null

test-cases/terraform/aws/networking/public_ec2_points_to_private_redshift/main.tf:114

Expected: aws_security_group[{{publicly_accessible_sg}}] description is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_security_group/main.tf:15

Expected: aws_security_group[{{default}}] description is defined and not null

test-cases/terraform/aws/best-practices/security_group_no_description_for_rules/main.tf:15

Expected: aws_security_group[{{default}}] description is defined and not null

Variable Without Description

Results **3**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All variables should contain a valid description.

test-cases/terraform/hcl_language_complexity/using_module_multi/mymodule/user.tf:9

Expected: 'description' is defined and not null

test-cases/terraform/hcl_language_complexity/using_module_multi/mymodule/user.tf:5

Expected: 'description' is defined and not null

test-cases/terraform/hcl_language_complexity/using_module_multi/mymodule/user.tf:1

Expected: 'description' is defined and not null

https://kics.io