KICS REPORT v1.5.1

HIGH	74	MEDIUM	53	LOW	21	INFO	43	TOTAL	191

PLATFORMS Terraform, Dockerfile, Common
START TIME 12:37:02, Nov 01 2022
END TIME 12:37:15, Nov 01 2022
SCANNED PATHS:
- .

AD Admin Not Configured For SQL Server

Results 1

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

The Active Directory Administrator is not configured for a SQL server

azure/sql.tf:9

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

App Service Managed Identity Disabled

Results 2

Severity HIGH
Platform Terraform
Category Resource Management

Description

Azure App Service should have managed identity enabled

azure/app_service.tf:22

Expected: 'azurerm_app_service[app-service1].identity' is defined and not null

azure/app_service.tf:43

Expected: 'azurerm_app_service[app-service2].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

azure/app_service.tf:29

Expected: 'azurerm_app_service[app-service1].site_config.min_tls_version' is set to '1.2'

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.

KICS REPORT v1.5.1

aws/iam.tf:29

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 **2**

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

Azure App Service client certificate should be enabled

azure/app_service.tf:43

Expected: 'azurerm_app_service[app-service2].client_cert_enabled' is defined

azure/app_service.tf:22

Expected: 'azurerm_app_service[app-service1].client_cert_enabled' is defined

BigQuery Dataset Is Public

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

BigQuery dataset is anonymously or publicly accessible

gcp/big_data.tf:24

Expected: 'access.special_group' is not equal to 'allAuthenticatedUsers'

CMK Rotation Disabled

Results **1**

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.

aws/kms.tf:1

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

COS Node Image Not Used

Results **1**

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

The node image should be Container-Optimized OS(COS)

gcp/gke.tf:29

KICS REPORT v1.5.1

Expected: 'node_config.image_type' should start with 'COS'

Client Certificate Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Clusters must be created with Client Certificate enabled, which means 'master_auth' must have 'client_certificate_config' with the attribute 'issue_client_certificate' equal to true

gcp/gke.tf:6

Expected: Attribute 'master_auth' is defined

Cloud Storage Bucket Logging Not Enabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Observability

Description

Cloud storage bucket with logging not enabled

gcp/gcs.tf:1

Expected: 'google_storage_bucket.logging' is set

Cloud Storage Bucket Versioning Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Observability

Description

Object Versioning Not Enabled on Cloud Storage Bucket

gcp/gcs.tf:1

Expected: 'versioning' is defined and not null

Cluster Labels Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Clusters must be configured with labels, which means the attribute 'resource_labels' must be defined

gcp/gke.tf:6

Expected: Attribute 'resource_labels' is defined

Cluster Master Authentication Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Engine Clusters must have Master Authentication set to enabled, which means the attribute 'master_auth' must have the subattributes 'username' and 'password' defined and not empty

gcp/gke.tf:6

KICS REPORT v1.5.1

Expected: Attribute 'master_auth' is defined

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').

aws/db-app.tf:21

Expected: 'publicly_accessible' is set to false or undefined

DB Instance Storage Not Encrypted

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

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

aws/db-app.tf:18

Expected: 'storage_encrypted' is set to true

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

aws/ec2.tf:53

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

EC2 Instance Has Public IP

Results 2

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

EC2 Instance should not have a public IP address.

aws/ec2.tf:1

Expected: 'associate_public_ip_address' is defined and not null

aws/db-app.tf:242

Expected: 'associate_public_ip_address' is defined and not null

EKS Cluster Encryption Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

EKS Cluster should be encrypted

aws/eks.tf:117

Expected: 'encryption_config' is defined and not null

GKE Basic Authentication Enabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

GCP - Google Kubernetes Engine (GKE) Basic Authentication must be disabled, which means the username and password provided in the master_auth block must be empty

gcp/gke.tf:6

Expected: Attribute 'master_auth' is defined

GKE Legacy Authorization Enabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Engine Clusters must have Legacy Authorization set to disabled, which means the attribute 'enable_legacy_abac' must not be true

gcp/gke.tf:12

Expected: Attribute 'enable_legacy_abac' is false

Geo Redundancy Is Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Backup

Description

Make sure that on PostgreSQL Geo Redundant Backups is enabled

azure/sql.tf:80

Expected: 'azurerm_postgresql_server.example.geo_redundant_backup_enabled' is true

HTTP Port Open

Results 1

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

The HTTP port is open in a Security Group

aws/ec2.tf:77

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

IAM Database Auth Not Enabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

IAM Database Auth Enabled must be configured to true

aws/db-app.tf:1

Expected: 'iam_database_authentication_enabled' is set to true

KICS REPORT v1.5.1

IP Aliasing Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Clusters must be created with Alias IP ranges enabled, which means the attribut 'ip_allocation_policy' must be defined and, if defined, the attribute 'networking_mode' must be VPC_NATIVE

gcp/gke.tf:6

Expected: Attributes 'ip_allocation_policy' and 'networking_mode' are defined

Key Expiration Not Set

Results 1

Severity	HIGH
Platform	Terraform
Category	Secret Management

Description

Make sure that for all keys the expiration date is set

azure/key_vault.tf:33

Expected: 'expiration_date' exists

Missing User Instruction

Results 1

Severity	HIGH
Platform	Dockerfile
Category	Build Process

Description

A user should be specified in the dockerfile, otherwise the image will run as root

aws/resources/Dockerfile:1

Expected: The 'Dockerfile' contains the 'USER' instruction

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

azure/sql.tf:60

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

azure/sql.tf:59

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

Network Policy Disabled

Results 1

KICS REPORT v1.5.1

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Kubernetes Engine Clusters must have Network Policy enabled, meaning that the attribute 'network_policy.enabled' must be true and the attribute 'addons_config.network_policy_config.disabled' must be false

gcp/gke.tf:6

Expected: Attribute 'network_policy' is defined and Attribute 'addons_config' is defined

Network Watcher Flow Disabled

Results **1**

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Check if enable field in the resource azurerm_network_watcher_flow_log is false.

azure/networking.tf:126

Expected: azurerm_network_watcher_flow_log.enabled is true

Node Auto Upgrade Disabled

Results **1**

Severity HIGH
Platform Terraform
Category Resource Management

Description

Node 'auto_upgrade' should be enabled for Kubernetes Clusters

gcp/gke.tf:24

Expected: google_container_node_pool.management is defined and not null

Passwords And Secrets - AWS Access Key

Results **3**

Severity HIGH
Platform Common
Category Secret Management

Description

Query to find passwords and secrets in infrastructure code.

aws/ec2.tf:15

Expected: Hardcoded secret key should not appear in source

aws/lambda.tf:44

Expected: Hardcoded secret key should not appear in source

aws/providers.tf:10

Expected: Hardcoded secret key should not appear in source

Passwords And Secrets - AWS Secret Key

Results **1**

Severity HIGH
Platform Common
Category Secret Management

Description

Query to find passwords and secrets in infrastructure code.

aws/ec2.tf:16

Expected: Hardcoded secret key should not appear in source

Passwords And Secrets - Generic Password

Results 2

Severity	HIGH
Platform	Common
Category	Secret Management

Description

Query to find passwords and secrets in infrastructure code.

azure/sql.tf:83

Expected: Hardcoded secret key should not appear in source

azure/sql.tf:15

Expected: Hardcoded secret key should not appear in source

Passwords And Secrets - Generic Secret

Results 2

Severity	HIGH
Platform	Common
Category	Secret Management

Description

Query to find passwords and secrets in infrastructure code.

aws/lambda.tf:45

Expected: Hardcoded secret key should not appear in source

aws/providers.tf:11

Expected: Hardcoded secret key should not appear in source

Pod Security Policy Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Kubernetes Clusters must have Pod Security Policy controller enabled, which means there must be a 'pod_security_policy_config' with the 'enabled' attribute equal to true

gcp/gke.tf:6

Expected: Attribute 'pod_security_policy_config' is defined

PostgreSQL Server Threat Detection Policy Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Resource Management

Description

PostgreSQL Server Threat Detection Policy should be enabled

azure/sql.tf:73

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

Private Cluster Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

KICS REPORT v1.5.1

Kubernetes Clusters must be created with Private Clusters enabled, meaning the 'private_cluster_config' must be defined and the attributes 'enable_private_nodes' and 'enable_private_endpoint' must be true

gcp/gke.tf:6

Expected: Attribute 'private_cluster_config' is defined and not null

S3 Bucket ACL Allows Read Or Write to All Users

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

S3 bucket with public READ/WRITE access

aws/s3.tf:7

Expected: 'acl' is equal 'private'

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.

aws/s3.tf:24

Expected: aws_s3_bucket_object.server_side_encryption is defined and not null

S3 Bucket SSE Disabled

Results **5**

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

aws/s3.tf:66

Expected: 'server_side_encryption_configuration' is defined and not null

aws/ec2.tf:271

Expected: 'server_side_encryption_configuration' is defined and not null

aws/s3.tf:91

Expected: 'server_side_encryption_configuration' is defined and not null

aws/s3.tf:1

Expected: 'server_side_encryption_configuration' is defined and not null

aws/s3.tf:43

Expected: 'server_side_encryption_configuration' is defined and not null

S3 Bucket Without Enabled MFA Delete

Results **6**

Severity	HIGH
Platform	Terraform

KICS REPORT v1.5.1

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.

aws/ec2.tf:271

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

aws/s3.tf:71

Expected: 'mfa_delete' is set to true

aws/s3.tf:43

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

aws/s3.tf:118

Expected: 'mfa_delete' is set to true

aws/s3.tf:95

Expected: 'mfa_delete' is set to true

aws/s3.tf:1

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

SQL DB Instance Backup Disabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Backup

Description

Checks if backup configuration is enabled for all Cloud SQL Database instances

gcp/big_data.tf:16

Expected: settings.backup_configuration.enabled is true

SQL DB Instance Is Publicly Accessible

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

Check if any Cloud SQL instances are publicly accessible.

gcp/big_data.tf:12

Expected: 'authorized_network' address is trusted

SQL DB Instance With SSL Disabled

Results **1**

Severity	HIGH
Platform	Terraform
Category	Encryption

Description

Cloud SQL Database Instance should have SLL enabled

gcp/big_data.tf:8

KICS REPORT v1.5.1

Expected: 'settings.ip_configuration.require_ssl' 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'

azure/sql.tf:85

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

Secret Expiration Not Set

Results 1

Severity	HIGH
Platform	Terraform
Category	Secret Management

Description

Make sure that for all secrets the expiration date is set

azure/key_vault.tf:58

Expected: 'expiration_date' exists

Security Group With Unrestricted Access To SSH

Results 1

Severity	HIGH
Platform	Terraform
Category	Networking and Firewall

Description

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

aws/ec2.tf:87

Expected: aws_security_group[web-node] 'SSH' (Port:22) is not public

Stackdriver Logging Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Observability

Description

Kubernetes Engine Clusters must have Stackdriver Logging enabled, which means the attribute 'logging_service' must be defined and different from 'none'

gcp/gke.tf:6

Expected: Attribute 'logging_service' is not 'none'

Stackdriver Monitoring Disabled

Results 1

Severity	HIGH
Platform	Terraform
Category	Observability

Description

Kubernetes Engine Clusters must have Stackdriver Monitoring enabled, which means the attribute 'monitoring_service' must be defined and different than 'none'

gcp/gke.tf:6

Expected: Attribute 'monitoring_service' is not 'none'

KICS REPORT v1.5.1

Storage Account Not Forcing HTTPS

Results 1

Severity HIGH
Platform Terraform
Category Encryption

Description

See that Storage Accounts forces the use of HTTPS

azure/storage.tf:23

Expected: 'azurerm_storage_account.example.enable_https_traffic_only' equals 'true'

Trusted Microsoft Services Not Enabled

Results 2

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

Trusted MIcrosoft Services are not enabled for Storage Account access

azure/storage.tf:23

Expected: 'network_rules' is defined and not null

azure/storage.tf:68

Expected: 'bypass' contains 'AzureServices'

Unknown Port Exposed To Internet

Results 1

Severity HIGH
Platform Terraform
Category Networking and Firewall

Description

AWS Security Group should not have an unknown port exposed to the entire Internet

aws/ec2.tf:87

Expected: aws_security_group[web-node].ingress.from_port is known

Unrestricted Security Group Ingress

Results 2

Severity HIGH
Platform Terraform
Category Networking and Firewall

Description

Security groups allow ingress from 0.0.0.0:0

aws/ec2.tf:88

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

aws/ec2.tf:95

Expected: One of 'ingress.cidr_blocks' not equal '0.0.0.0/0'

Vault Auditing Disabled

Results 1

Severity HIGH
Platform Terraform
Category Observability

Description

Ensure that logging for Azure KeyVault is 'Enabled'

azure/key_vault.tf:1

KICS REPORT v1.5.1

Expected: 'azurerm_key_vault' is associated with 'azurerm_monitor_diagnostic_setting'

Web App Accepting Traffic Other Than HTTPS

Results 1

Severity	HIGH
Platform	Terraform
Category	Insecure Configurations

Description

Web app should only accept HTTPS traffic in Azure Web App Service.

azure/app_service.tf:27

Expected: 'azurerm_app_service[app-service1].https_only' is set to true

AKS Disk Encryption Set ID Undefined

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Azure Container Service (AKS) should use Disk Encryption Set ID

azure/aks.tf:1

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].disk_encryption_set_id' is defined and not null

AKS Network Policy Misconfigured

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Check if the Azure Kubernetes Service doesn't have the proper network policy configuration.

azure/aks.tf:1

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].network_profile' is set

AKS RBAC Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Azure Container Service (AKS) instance should have role-based access control (RBAC) enabled

azure/aks.tf:23

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].role_based_access_control.enabled' is set to true

Cloud Storage Anonymous or Publicly Accessible

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

Cloud Storage Buckets must not be anonymously or publicly accessible, which means the attribute 'members' must not possess 'allUsers' or 'allAuthenticatedUsers'

gcp/gcs.tf:18

Expected: 'google_storage_bucket_iam_binding[allow_public_read].members' does not have 'allUsers'

KICS REPORT v1.5.1

Disk Encryption Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

VM disks for critical VMs must be encrypted with Customer Supplied Encryption Keys (CSEK) or with Customer-managed encryption keys (CMEK), which means the attribute 'disk_encryption_key' must be defined and its sub attributes 'raw_key' or 'kms_key_self_link' must also be defined

gcp/instances.tf:36

Expected: 'google_compute_disk[unencrypted_disk].disk_encryption_key' is defined and not null

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.

aws/ec2.tf:34

Expected: One of 'aws_ebs_volume.encrypted' is defined

ECR Image Tag Not Immutable

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

ECR should have an image tag be immutable

aws/ecr.tf:3

Expected: aws_ecr_repository.repository.image_tag_mutability is 'IMMUTABLE'

ECR Repository Not Encrypted

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

ECR (Elastic Container Registry) Repository encryption should be set

aws/ecr.tf:1

Expected: The attribute 'encryption_configuration' is defined and not null

ElasticSearch Not Encrypted At Rest

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

https://kics.io

KICS REPORT v1.5.1

Check if ElasticSearch encryption is disabled at Rest

aws/es.tf:1

Expected: 'encrypt_at_rest' is set and enabled

Elasticsearch Domain Not Encrypted Node To Node

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Elasticsearch Domain encryption should be enabled node to node

aws/es.tf:1

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'.

aws/es.tf:42

Expected: aws_elasticsearch_domain_policy[monitoring-framework-policy].access_policies does not have wildcard in 'Action' and 'Principal'

Elasticsearch Log is disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

AWS Elasticsearch should have logs enabled

aws/es.tf:1

Expected: 'log_publishing_options' is defined and not null

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

azure/security_center.tf:6

Expected: 'azurerm_security_center_contact.contact.alert_notifications' is true

Encryption On Managed Disk Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Ensure that the encryption is active on the disk

azure/storage.tf:9

KICS REPORT v1.5.1

Expected: azurerm_managed_disk[example].encryption_settings.enabled is true

Google Compute Network Using Firewall Rule that Allows All Ports

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

Google Compute Network should not use a firewall rule that allows all ports

gcp/networks.tf:1

Expected: 'google_compute_network[vpc]' is not using a firewall rule that allows access to all ports

Google Compute Subnetwork Logging Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Observability

Description

This query checks if logs are enabled for a Google Compute Subnetwork resource.

gcp/networks.tf:7

Expected: 'google_compute_subnetwork[public-subnetwork].log_config' is defined and not null

Google Container Node Pool Auto Repair Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Verifies if Google Container Node Pool Auto Repair is Enabled

gcp/gke.tf:24

Expected: google_container_node_pool[custom_node_pool].management.auto_repair is defined and not null

Google Storage Bucket Level Access Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Insecure Configurations

Description

Google Storage Bucket Level Access should be enabled

gcp/gcs.tf:1

Expected: google_storage_bucket[terragoat_website].uniform_bucket_level_access is defined and not null

IAM Access Analyzer Undefined

Results 1

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

IAM Access Analyzer should be defined to identify unintentional access

aws/db-app.tf:1

Expected: 'aws_accessanalyzer_analyzer' is set

IAM Access Key Is Exposed

Results 1

KICS REPORT v1.5.1

Severity	MEDIUM
Platform	Terraform
Category	Access Control
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 1.11
Title	Do not setup access keys during initial user setup for all IAM users that have a console password

Description

AWS console defaults to no check boxes selected when creating a new IAM user. When cerating the IAM User credentials you have to determine what type of access they require. Programmatic access: The IAM user might need to make API calls, use the AWS CLI, or use the Tools for Windows PowerShell. In that case, create an access key (access key ID and a secret access key) for that user. AWS Management Console access: If the user needs to access the AWS Management Console, create a password for the user. Requiring the additional steps be taken by the user for programmatic access after their profile has been created will give a stronger indication of intent that access keys are [a] necessary for their work and [b] once the access key is established on an account that the keys may be in use somewhere in the organization. Note : Even if it is known the user will need access keys, require them to create the keys themselves or put in a support ticket to have them created as a separate step from user creation.

aws/iam.tf:21

Expected: 'aws_iam_access_key[user].user' is 'root' for an active access key

IAM Policy Grants Full Permissions

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Access Control

Description

IAM policies allow all ('*') in a statement action

aws/iam.tf:29

Expected: 'policy.Statement.Resource' not equal '*'

aws/db-app.tf:209

Expected: 'policy.Statement.Resource' not equal '*'

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

aws/neptune.tf:7

Expected: 'iam_database_authentication_enabled' is set to true

Neptune Database Cluster Encryption Disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

Check if Neptune Cluster Storage is securely encrypted

aws/neptune.tf:9

Expected: 'storage_encrypted' should be true

KICS REPORT v1.5.1

OSLogin Is Disabled For VM Instance

Results 1

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Check if any VM instance disables OSLogin

gcp/instances.tf:21

Expected: google_compute_instance[server].metadata.enable-oslogin is true or undefined

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'

azure/sql.tf:109

Expected: 'azurerm_postgresql_configuration.example.value' should be 'ON'

PostgreSQL Server Without Connection Throttling

Results 1

Severity MEDIUM
Platform Terraform
Category Observability

Description

Ensure that Connection Throttling is set for the PostgreSQL server

azure/sql.tf:102

Expected: 'azurerm_postgresql_configuration.thrtottling_config.value' should be 'ON'

Project-wide SSH Keys Are Enabled In VM Instances

Results 1

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

VM Instance should block project-wide SSH keys

gcp/instances.tf:20

Expected: google_compute_instance[server].metadata.block-project-ssh-keys is true

RDP Access Is Not Restricted

Results 1

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

Check if Google Firewall ingress allows RDP access (port 3389)

gcp/networks.tf:25

Expected: 'google_compute_firewall[allow_all].allow.ports' does not include RDP port 3389

RDS With Backup Disabled

Results 1

Severity MEDIUM

KICS REPORT v1.5.1

Platform Terraform
Category Backup

Description

RDS configured without backup

aws/db-app.tf:17

Expected: 'backup_retention_period' is not equal '0'

Role Definition Allows Custom Role Creation

Results **1**

Severity MEDIUM
Platform Terraform
Category Access Control

Description

Role Definition should not allow custom role creation

azure/roles.tf:9

Expected: azurerm_role_definition[example].permissions.actions does not allow custom role creation

S3 Bucket Without Versioning

Results **3**

Severity MEDIUM
Platform Terraform
Category Observability

Description

S3 bucket should have versioning enabled

aws/s3.tf:1

Expected: 'versioning' is set to true

aws/s3.tf:43

Expected: 'versioning' is set to true

aws/ec2.tf:271

Expected: 'versioning' is set to true

SQL Server Auditing Disabled

Results **1**

Severity MEDIUM
Platform Terraform
Category Observability

Description

Make sure that for SQL Servers, 'Auditing' is set to 'On'

azure/sql.tf:9

Expected: 'azurerm_sql_server.example.extended_auditing_policy' exists

SSH Access Is Not Restricted

Results **1**

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

Check if Google Firewall allows SSH access (port 22) from the Internet (public CIDR block)

gcp/networks.tf:25

Expected: 'google_compute_firewall[allow_all].allow.ports' does not include SSH port 22

Security Center Pricing Tier Is Not Standard

Results **1**

KICS REPORT v1.5.1

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Make sure that the 'Standard' pricing tiers were selected.

azure/security_center.tf:2

Expected: 'azurerm_security_center_subscription_pricing.pricing.tier' is 'Standard'

Serial Ports Are Enabled For VM Instances

Results **1**

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Check if VM instance enables serial ports

gcp/instances.tf:22

Expected: google_compute_instance[server].metadata.serial-port-enable is false or undefined

Small Activity Log Retention Period

Results **1**

Severity MEDIUM
Platform Terraform
Category Observability

Description

Ensure that Activity Log Retention is set 365 days or greater

azure/logging.tf:8

Expected: 'azurerm_monitor_log_profile[logging_profile].retention_policy.days' is greater than or equal to 365 days or 0 (indefinitely)

Small Flow Logs Retention Period

Results **2**

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Flow logs enable capturing information about IP traffic flowing in and out of the network security groups. Network Security Group Flow Logs must be enabled with retention period greater than or equal to 90 days. This is important, because these logs are used to check for anomalies and give information of suspected breaches

azure/networking.tf:133

Expected: 'flow_log.retention_policy.days' is bigger than 90)

azure/networking.tf:132

Expected: 'flow_log.retention_policy' should be enabled)

Storage Account Not Using Latest TLS Encryption Version

Results **1**

Severity MEDIUM
Platform Terraform
Category Encryption

Description

Ensure Storage Account is using the latest version of TLS encryption

azure/storage.tf:23

Expected: 'azurerm_storage_account[example].min_tls_version' is defined and not null

KICS REPORT v1.5.1

Unscanned ECR Image

Results 1

Severity MEDIUM
Platform Terraform
Category Encryption

Description

Checks if the ECR Image has been scanned

aws/ecr.tf:1

Expected: aws_ecr_repository[repository].image_scanning_configuration is defined

Using Default Service Account

Results 1

Severity MEDIUM
Platform Terraform
Category Insecure Configurations

Description

Instances must not be configured to use the Default Service Account, that has full access to all Cloud APIs, which means the attribute 'service_account' and its sub attribute 'email' must be defined. Additionally, 'email' must not be empty and must also not be a default Google Compute Engine service account.

gcp/instances.tf:3

Expected: 'google_compute_instance[server].service_account' is defined and not null

VPC FlowLogs Disabled

Results 1

Severity MEDIUM
Platform Terraform
Category Observability

Description

VPC hasn't got any FlowLog associated

aws/eks.tf:43

Expected: aws_vpc[eks_vpc] is the same as Flow Logs VPC id

VPC Subnet Assigns Public IP

Results 4

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

Description

VPC Subnet should not assign public IP

aws/eks.tf:93

Expected: aws_subnet[eks_subnet2].map_public_ip_on_launch is set to false or undefined

aws/ec2.tf:139

Expected: aws_subnet[web_subnet].map_public_ip_on_launch is set to false or undefined

aws/ec2.tf:159

Expected: aws_subnet[web_subnet2].map_public_ip_on_launch is set to false or undefined

aws/eks.tf:65

Expected: aws_subnet[eks_subnet1].map_public_ip_on_launch is set to false or undefined

VPC Without Network Firewall

Results 2

Severity MEDIUM
Platform Terraform
Category Networking and Firewall

KICS REPORT v1.5.1

Description

VPC should have a Network Firewall associated

aws/ec2.tf:117

Expected: aws_vpc[web_vpc] has an 'aws_networkfirewall_firewall' associated

aws/eks.tf:43

Expected: aws_vpc[eks_vpc] has an 'aws_networkfirewall_firewall' associated

Virtual Network with DDoS Protection Plan disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Availability

Description

Virtual Network should have DDoS Protection Plan enabled

azure/networking.tf:1

Expected: 'azurerm_virtual_network[example].ddos_protection_plan' is defined and not null

WAF Is Disabled For Azure Application Gateway

Results **1**

Severity	MEDIUM
Platform	Terraform
Category	Networking and Firewall

Description

Check if Web Application Firewall is disabled or not configured for Azure's Application Gateway.

azure/application_gateway.tf:1

Expected: 'azurerm_application_gateway[network]' is set

AKS Private Cluster Disabled

Results **1**

Severity	LOW
Platform	Terraform
Category	Networking and Firewall

Description

Azure Kubernetes Service (AKS) API should not be exposed to the internet

azure/aks.tf:1

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].private_cluster_enabled' is defined and set to true

AKS Uses Azure Policies Add-On Disabled

Results **1**

Severity	LOW
Platform	Terraform
Category	Best Practices

Description

Azure Container Service (AKS) should use Azure Policies Add-On

azure/aks.tf:14

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].addon_profile.azure_policy' is defined and set to true

App Service HTTP2 Disabled

Results **2**

Severity	LOW
Platform	Terraform
Category	Insecure Configurations

KICS REPORT v1.5.1

Description

App Service should have 'http2_enabled' enabled

azure/app_service.tf:43

Expected: 'azurerm_app_service[app-service2].site_config' is defined and not null

azure/app_service.tf:28

Expected: 'azurerm_app_service[app-service1].site_config.http2_enabled' is defined and not null

Dashboard Is Enabled

Results **1**

Severity	LOW
Platform	Terraform
Category	Insecure Configurations

Description

Check if the Kubernetes Dashboard is enabled.

azure/aks.tf:19

Expected: 'azurerm_kubernetes_cluster[k8s_cluster].addon_profile.kube_dashboard.enabled' is false or undefined

EC2 Instance Using API Keys

Results **2**

Severity	LOW
Platform	Terraform
Category	Access Control

Description

EC2 instances should use roles to be granted access to other AWS services

aws/db-app.tf:242

Expected: aws_instance[db_app] should be using iam_instance_profile to assign a role with permissions

aws/ec2.tf:1

Expected: aws_instance[web_host] should be using iam_instance_profile to assign a role with permissions

ECR Repository Without Policy

Results **1**

Severity	LOW
Platform	Terraform
Category	Best Practices

Description

ECR Repository should have Policies attached to it

aws/ecr.tf:1

Expected: aws_ecr_repository[repository] has policies attached

EKS cluster logging is not enabled

Results **1**

Severity	LOW
Platform	Terraform
Category	Observability

Description

Amazon EKS control plane logging is not enabled

aws/eks.tf:117

Expected: 'enabled_cluster_log_types' is defined and not null

Google Compute Subnetwork with Private Google Access Disabled

Results **1**

Severity	LOW
Platform	Terraform

https://kics.io

KICS REPORT v1.5.1

Category Networking and Firewall

Description

Google Compute Subnetwork should have 'private_ip_google_access' set to true

gcp/networks.tf:7

Expected: 'google_compute_subnetwork[public-subnetwork].private_ip_google_access' is defined and not null

Hardcoded AWS Access Key

Results **1**

Severity LOW
Platform Terraform
Category Secret Management

Description

Hard-coded AWS access key / secret key exists in EC2 user data

aws/ec2.tf:9

Expected: 'user_data' doesn't contain hardcoded access key

Healthcheck Instruction Missing

Results **1**

Severity LOW
Platform Dockerfile
Category Insecure Configurations

Description

Ensure that HEALTHCHECK is being used. The HEALTHCHECK instruction tells Docker how to test a container to check that it is still working

aws/resources/Dockerfile:1

Expected: Dockerfile contains instruction 'HEALTHCHECK'

IAM Policies Attached To User

Results **1**

Severity LOW
Platform Terraform
Category Best Practices

Description

IAM policies should be attached only to groups or roles

aws/iam.tf:27

Expected: 'user' is redundant

Key Vault Secrets Content Type Undefined

Results **1**

Severity LOW
Platform Terraform
Category Best Practices

Description

Key Vault Secrets should have set Content Type

azure/key_vault.tf:58

Expected: 'azurerm_key_vault_secret[secret].content_type' is defined and not null

Lambda Functions Without X-Ray Tracing

Results **1**

Severity LOW
Platform Terraform
Category Observability

Description

https://kics.io

KICS REPORT v1.5.1

AWS Lambda functions should have TracingConfig enabled. For this, property 'tracing_Config.mode' should have the value 'Active'

aws/lambda.tf:31

Expected: aws_lambda_function[analysis_lambda].tracing_config is defined and not null

PostgreSQL Server Infrastructure Encryption Disabled

Results **1**

Severity	LOW
Platform	Terraform
Category	Encryption

Description

PostgreSQL Server Infrastructure Encryption should be enabled

azure/sql.tf:73

Expected: 'azurerm_postgresql_server[example].infrastructure_encryption_enabled' is defined and set to true

S3 Bucket Logging Disabled

Results **5**

Severity	LOW
Platform	Terraform
Category	Observability

Description

S3 bucket without logging

aws/s3.tf:115

Expected: 'logging' is defined and not null

aws/s3.tf:43

Expected: 'logging' is defined and not null

aws/s3.tf:1

Expected: 'logging' is defined and not null

aws/s3.tf:66

Expected: 'logging' is defined and not null

aws/ec2.tf:271

Expected: 'logging' is defined and not null

App Service Authentication Disabled

Results **2**

Severity	INFO
Platform	Terraform
Category	Access Control

Description

Azure App Service authentication settings should be enabled

azure/app_service.tf:51

Expected: 'azurerm_app_service[app-service2].auth_settings.enabled' is true

azure/app_service.tf:22

Expected: 'azurerm_app_service[app-service1].auth_settings' is defined

EC2 Instance Monitoring Disabled

Results **2**

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

KICS REPORT v1.5.1

aws/ec2.tf:1

Expected: 'monitoring' is defined and not null%!(EXTRA string=web_host)

aws/db-app.tf:242

Expected: 'monitoring' is defined and not null%!(EXTRA string=db_app)

EC2 Not EBS Optimized

Results **2**

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

aws/db-app.tf:242

Expected: 'ebs_optimized' is set to true

aws/ec2.tf:1

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

aws/elb.tf:2

Expected: 'aws_elb[{{weblb}}].access_logs' is defined and not null

Name Is Not Snake Case

Results **10**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All names should follow snake case pattern.

aws/eks.tf:33

Expected: All names should be on snake case pattern

azure/app_service.tf:22

Expected: All names should be on snake case pattern

azure/policies.tf:1

Expected: All names should be on snake case pattern

aws/ec2.tf:231

Expected: All names should be on snake case pattern

gcp/networks.tf:7

Expected: All names should be on snake case pattern

azure/app_service.tf:43

Expected: All names should be on snake case pattern

aws/es.tf:40

Expected: All names should be on snake case pattern

KICS REPORT v1.5.1

aws/ec2.tf:77

Expected: All names should be on snake case pattern

aws/eks.tf:38

Expected: All names should be on snake case pattern

aws/es.tf:1

Expected: All names should be on snake case pattern

Neptune Logging Is Disabled

Results 1

Severity	INFO
Platform	Terraform
Category	Observability

Description

Neptune logging should be enabled

aws/neptune.tf:1

Expected: aws_neptune_cluster.enable_cloudwatch_logs_exports is defined

Output Without Description

Results 4

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All outputs should contain a valid description.

aws/iam.tf:48

Expected: 'description' is defined and not null

aws/iam.tf:52

Expected: 'description' is defined and not null

aws/eks.tf:146

Expected: 'description' is defined and not null

aws/eks.tf:142

Expected: 'description' is defined and not null

RDS Without Logging

Results 1

Severity	INFO
Platform	Terraform
Category	Observability

Description

RDS does not have any kind of logger

aws/db-app.tf:1

Expected: 'enabled_cloudwatch_logs_exports' is defined

Resource Not Using Tags

Results 2

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

AWS services resource tags are an essential part of managing components

aws/eks.tf:66

Expected: aws_subnet[{{eks_subnet1}}].tags has tags defined other than 'Name'

aws/eks.tf:94

Expected: aws_subnet[{{eks_subnet2}}].tags has tags defined other than 'Name'

SQL Server Alert Email Disabled

Results 1

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

SQL Server alert email should be enabled

azure/sql.tf:31

Expected: 'azurerm_mssql_server_security_alert_policy[example].email_account_admins' is defined

Security Group Rules Without Description

Results 3

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

aws/ec2.tf:90

Expected: aws_security_group[{{web-node}}].ingress description is defined and not null

aws/ec2.tf:83

Expected: aws_security_group[{{web-node}}].ingress description is defined and not null

aws/ec2.tf:97

Expected: aws_security_group[{{web-node}}].egress description is defined and not null

Security Group Without Description

Results 1

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

It's considered a best practice for AWS Security Group to have a description

aws/db-app.tf:116

Expected: aws_security_group[{{default}}] description is defined and not null

Variable Without Description

Results 7

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All variables should contain a valid description.

gcp/variables.tf:11

Expected: 'description' is defined and not null

aws/consts.tf:4

Expected: 'description' is defined and not null

aws/consts.tf:28

Expected: 'description' is defined and not null

aws/consts.tf:20

Expected: 'description' is defined and not null

aws/consts.tf:8

Expected: 'description' is defined and not null

aws/consts.tf:24

Expected: 'description' is defined and not null

azure/variables.tf:7

Expected: 'description' is defined and not null

Variable Without Type

Results **6**

Severity	INFO
Platform	Terraform
Category	Best Practices

Description

All variables should contain a valid type.

azure/variables.tf:12

Expected: 'type' is defined and not null

aws/consts.tf:24

Expected: 'type' is defined and not null

aws/consts.tf:8

Expected: 'type' is defined and not null

aws/consts.tf:4

Expected: 'type' is defined and not null

gcp/variables.tf:16

Expected: 'type' is defined and not null

aws/consts.tf:20

Expected: 'type' is defined and not null