KICS REPORT v1.4.9

HIGH	11	MEDIUM	4	LOW	2	INFO	14	TOTAL	31

PLATFORMS	Common, Terraform
START TIME	00:05:58, Feb 24 2022
END TIME	00:06:14, Feb 24 2022

SCANNED PATHS:

- git::https://github.com/superaims/infoseccapstone/

Passwords And Secrets - AWS Access Key

Results **1**

Severity	HIGH
Platform	Common
Category	Secret Management

Description

Query to find passwords and secrets in infrastructure code.

git::https://github.com/superaims/infoseccapstone//providers.tf:10

Expected: Hardcoded secret key should not appear in source

Passwords And Secrets - Generic Secret

Results **1**

Severity	HIGH
Platform	Common
Category	Secret Management

Description

Query to find passwords and secrets in infrastructure code.

git::https://github.com/superaims/infoseccapstone//providers.tf:11

Expected: Hardcoded secret key should not appear in source

S3 Bucket Access to Any Principal

Results **1**

Severity	HIGH
Platform	Terraform
Category	Access Control

Description

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

git::https://github.com/superaims/infoseccapstone//main.tf:72

Expected: aws_s3_bucket_policy[public].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.

git::https://github.com/superaims/infoseccapstone//main.tf:78

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

S3 Bucket Object Not Encrypted

Results **2**

Severity	HIGH
Platform	Terraform
Category	Encryption
CIS ID	CIS Security - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Rule 2.1.1
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.

git::https://github.com/superaims/infoseccapstone//main.tf:111

Expected: aws_s3_bucket_object.server_side_encryption is defined and not null

git::https://github.com/superaims/infoseccapstone//main.tf:103

Expected: aws_s3_bucket_object.server_side_encryption is defined and not null

S3 Bucket SSE Disabled

Results **2**

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

git::https://github.com/superaims/infoseccapstone//main.tf:15

Expected: 'server_side_encryption_configuration' is defined and not null

git::https://github.com/superaims/infoseccapstone//main.tf:5

Expected: 'server_side_encryption_configuration' is defined and not null

S3 Bucket Without Enabled MFA Delete

Results **3**

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.

git::https://github.com/superaims/infoseccapstone//main.tf:40

Expected: 'mfa_delete' is set to true

git::https://github.com/superaims/infoseccapstone//main.tf:41

Expected: 'enabled' is set to true

git::https://github.com/superaims/infoseccapstone//main.tf:5

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

S3 Bucket Policy Accepts HTTP Requests

Results **2**

Severity	MEDIUM
Platform	Terraform
Category	Encryption

Description

S3 Bucket policy should not accept HTTP Requests

git::https://github.com/superaims/infoseccapstone//main.tf:49

Expected: aws_s3_bucket_policy[private].policy does not accept HTTP Requests

git::https://github.com/superaims/infoseccapstone//main.tf:72

Expected: aws_s3_bucket_policy[public].policy does not accept HTTP Requests

S3 Bucket Without Versioning

Results **2**

Severity MEDIUM
Platform Terraform
Category Observability

Description

S3 bucket without versioning

git::https://github.com/superaims/infoseccapstone//main.tf:5

Expected: 'versioning' is set to true

git::https://github.com/superaims/infoseccapstone//main.tf:41

Expected: 'versioning.enabled' is set to true

S3 Bucket Logging Disabled

Results **2**

Severity LOW
Platform Terraform
Category Observability

Description

S3 bucket without logging

git::https://github.com/superaims/infoseccapstone//main.tf:15

Expected: 'logging' is defined and not null

git::https://github.com/superaims/infoseccapstone//main.tf:5

Expected: 'logging' is defined and not null

Resource Not Using Tags

Results **3**

Severity INFO
Platform Terraform
Category Best Practices

Description

AWS services resource tags are an essential part of managing components

git::https://github.com/superaims/infoseccapstone//main.tf:19

Expected: aws_s3_bucket[{{this}}].tags has tags defined other than 'Name'

git::https://github.com/superaims/infoseccapstone//main.tf:111

Expected: aws_s3_bucket_object[{{base64_file}}].tags is defined and not null

git::https://github.com/superaims/infoseccapstone//main.tf:103

Expected: aws_s3_bucket_object[{{file}}].tags is defined and not null

Variable Without Type

Results **11**

Severity INFO
Platform Terraform
Category Best Practices

Description

All variables should contain a valid type.

git::https://github.com/superaims/infoseccapstone//variables.tf:30

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:1

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:50

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:9

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:55

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:40

Expected: 'type' is defined and not null git::https://github.com/superaims/infoseccapstone//variables.tf:45

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:5

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:60

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:35

Expected: 'type' is defined and not null

git::https://github.com/superaims/infoseccapstone//variables.tf:25

Expected: 'type' is defined and not null