Checkmarx

KICS REPORT v2.1.1

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
2	13	103	11	31	160

PLATFORMS Terraform, Common
START TIME 14:00:42, Jul 24 2024
END TIME 14:00:53, Jul 24 2024
SCANNED PATHS:
- /path/modules/module-1/main.tf

S3 Bucket ACL Allows Read Or Write to All Users

Results 2

Severity CRITICAL
Platform Terraform
Cwe
Category Access Control

Description

S3 Buckets should not be readable and writable to all users

../../path/modules/module-1/main.tf:3311

Expected: aws_s3_bucket_acl[dev].acl should be private

../../path/modules/module-1/main.tf:3388

Expected: aws_s3_bucket_acl[bucket_temp].acl should be private

DynamoDB Table Not Encrypted

Results 2

Severity HIGH
Platform Terraform
Cwe
Category Encryption

Description

AWS DynamoDB Tables should have server-side encryption

../../path/modules/module-1/main.tf:3608

Expected: aws_dynamodb_table.server_side_encryption.enabled should be set to true

../../path/modules/module-1/main.tf:3620

Expected: aws_dynamodb_table.server_side_encryption.enabled should be set to true

Passwords And Secrets - Generic Secret

Results 1

Severity HIGH
Platform Common
Cwe
Category Secret Management

Description

Query to find passwords and secrets in infrastructure code.

../../path/modules/module-1/main.tf:3094

Expected: Hardcoded secret key should not appear in source

S3 Bucket Allows Public Policy

Results 3

Severity HIGH
Platform Terraform
Cwe
Category Access Control

Checkmarx

KICS REPORT v2.1.1

Description
S3 bucket allows public policy

../../path/modules/module-1/main.tf:3208

Expected: 'block_public_policy' should equal 'true'

../../path/modules/module-1/main.tf:3369

Expected: 'block_public_policy' should equal 'true'

../../path/modules/module-1/main.tf:3292

Expected: 'block_public_policy' should equal 'true'

S3 Bucket Object Not Encrypted

Results **5**

Severity	HIGH
Platform	Terraform
Cwe	
Category	Encryption

Description
S3 Bucket Object should have server-side encryption enabled

../../path/modules/module-1/main.tf:3264

Expected: aws_s3_bucket_object.server_side_encryption should be defined and not null

../../path/modules/module-1/main.tf:3332

Expected: aws_s3_bucket_object.server_side_encryption should be defined and not null

../../path/modules/module-1/main.tf:3392

Expected: aws_s3_bucket_object.server_side_encryption should be defined and not null

../../path/modules/module-1/main.tf:3341

Expected: aws_s3_bucket_object.server_side_encryption should be defined and not null

../../path/modules/module-1/main.tf:3401

Expected: aws_s3_bucket_object.server_side_encryption should be defined and not null

Sensitive Port Is Exposed To Entire Network

Results **1**

Severity	HIGH
Platform	Terraform
Cwe	
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

../../path/modules/module-1/main.tf:3464

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

Unrestricted Security Group Ingress

Results **1**

Severity	HIGH
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description
Security groups allow ingress from 0.0.0.0:0 and/or ::/0

../../path/modules/module-1/main.tf:3468

Checkmarx

KICS REPORT v2.1.1

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

API Gateway Access Logging Disabled

Results **2**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

Description

API Gateway Stage should have Access Logging Settings defined

../../path/modules/module-1/main.tf:160

Expected: 'access_log_settings' should be defined

../../path/modules/module-1/main.tf:160

Expected: aws_api_gateway_stage[api]'s corresponding aws_api_gateway_method_settings should be defined and not null

API Gateway Deployment Without Access Log Setting

Results **2**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

Description

API Gateway Deployment should have access log setting defined when connected to an API Gateway Stage.

../../path/modules/module-1/main.tf:154

Expected: aws_api_gateway_deployment[api] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

../../path/modules/module-1/main.tf:2931

Expected: aws_api_gateway_deployment[apideploy_ba] has a 'aws_api_gateway_stage' resource associated with 'access_log_settings' set

API Gateway Endpoint Config is Not Private

Results **2**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description

The API Endpoint type in API Gateway should be set to PRIVATE so it's not exposed to the public internet

../../path/modules/module-1/main.tf:70

Expected: 'aws_api_gateway_rest_api.aws_api_gateway_rest_api.types' should be 'PRIVATE'.

../../path/modules/module-1/main.tf:177

Expected: 'aws_api_gateway_rest_api.aws_api_gateway_rest_api.types' should be 'PRIVATE'.

API Gateway Method Does Not Contains An API Key

Results **42**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Access Control

Description

An API Key should be required on a method request.

Checkmarx

KICS REPORT v2.1.1

../../path/modules/module-1/main.tf:321

Expected: resource.aws_api_gateway_method[proxy_ban_user_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:2804

Expected: resource.aws_api_gateway_method[proxy_change_profile_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:2144

Expected: resource.aws_api_gateway_method[proxy_user_details_modal_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1041

Expected: resource.aws_api_gateway_method[register_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:877

Expected: resource.aws_api_gateway_method[proxy_login_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1616

Expected: resource.aws_api_gateway_method[proxy_search_author_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:901

Expected: resource.aws_api_gateway_method[login_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:742

Expected: resource.aws_api_gateway_method[proxy_list_posts_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1017

Expected: resource.aws_api_gateway_method[proxy_register_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1771

Expected: resource.aws_api_gateway_method[reset_password_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:625

Expected: resource.aws_api_gateway_method[dump_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2168

Expected: resource.aws_api_gateway_method[user_details_modal_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:215

Expected: resource.aws_api_gateway_method[xss_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2409

Expected: resource.aws_api_gateway_method[proxy_change_auth_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:2672

Expected: resource.aws_api_gateway_method[proxy_get_dashboard_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1508

Expected: resource.aws_api_gateway_method[proxy_save_content_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:767

Expected: resource.aws_api_gateway_method[list_posts_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:1878

Expected: resource.aws_api_gateway_method[proxy_get_users_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:2277

Expected: resource.aws_api_gateway_method[proxy_delete_user_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1746

Expected: resource.aws_api_gateway_method[proxy_reset_password_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:2301

Expected: resource.aws_api_gateway_method[delete_user_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:483

Expected: resource.aws_api_gateway_method[change_password_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:1903

Checkmarx

KICS REPORT v2.1.1

Expected: resource.aws_api_gateway_method[get_users_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:1450

Expected: resource.aws_api_gateway_method[save_content_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2565

Expected: resource.aws_api_gateway_method[modify_post_status_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2541

Expected: resource.aws_api_gateway_method[proxy_modify_post_status_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:345

Expected: resource.aws_api_gateway_method[ban_user_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:82

Expected: resource.aws_api_gateway_method[endpoint].api_key_required should be defined

../../path/modules/module-1/main.tf:192

Expected: resource.aws_api_gateway_method[proxy_xss_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1312

Expected: resource.aws_api_gateway_method[verify_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2828

Expected: resource.aws_api_gateway_method[change_profile_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:600

Expected: resource.aws_api_gateway_method[proxy_dump_root_get].api_key_required should be defined

../../path/modules/module-1/main.tf:1640

Expected: resource.aws_api_gateway_method[search_author_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2433

Expected: resource.aws_api_gateway_method[change_auth_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2696

Expected: resource.aws_api_gateway_method[get_dashboard_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:1426

Expected: resource.aws_api_gateway_method[proxy_save_content_root_get].api_key_required should be defined

../../path/modules/module-1/main.tf:2034

Expected: resource.aws_api_gateway_method[unban_user_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:1151

Expected: resource.aws_api_gateway_method[proxy_save_post_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1288

Expected: resource.aws_api_gateway_method[proxy_verify_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:459

Expected: resource.aws_api_gateway_method[proxy_change_password_root_post].api_key_required should be defined

../../path/modules/module-1/main.tf:1175

Expected: resource.aws_api_gateway_method[save_post_root_options].api_key_required should be defined

../../path/modules/module-1/main.tf:2010

Expected: resource.aws_api_gateway_method[proxy_unban_user_root_post].api_key_required should be defined

API Gateway With CloudWatch Logging Disabled

Results **1**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

https://kics.io

Checkmarx

KICS REPORT v2.1.1

Description

AWS CloudWatch Logs for APIs should be enabled and using the naming convention described in documentation

../../path/modules/module-1/main.tf:160

Expected: 'aws_cloudwatch_log_group' should be defined and use the correct naming convention

API Gateway With Open Access

Results **22**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Insecure Configurations

Description

API Gateway Method should restrict the authorization type, except for the HTTP OPTIONS method.

../../path/modules/module-1/main.tf:85

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2147

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1020

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:324

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2807

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1291

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2675

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2280

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1619

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:603

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:880

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2013

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:2412

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:745

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1881

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:195

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

Checkmarx

KICS REPORT v2.1.1

../../path/modules/module-1/main.tf:2544

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:462

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1749

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1429

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1154

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

../../path/modules/module-1/main.tf:1511

Expected: aws_api_gateway_method.authorization should only be 'NONE' if http_method is 'OPTIONS'

API Gateway Without Configured Authorizer

Results **2**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Access Control

Description

API Gateway REST API should have an API Gateway Authorizer

../../path/modules/module-1/main.tf:172

Expected: API Gateway REST API should be associated with an API Gateway Authorizer

../../path/modules/module-1/main.tf:66

Expected: API Gateway REST API should be associated with an API Gateway Authorizer

API Gateway Without SSL Certificate

Results **1**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Insecure Configurations

Description

SSL Client Certificate should be enabled

../../path/modules/module-1/main.tf:160

Expected: Attribute 'client_certificate_id' should be set

API Gateway without WAF

Results **1**

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description

API Gateway should have WAF (Web Application Firewall) enabled

../../path/modules/module-1/main.tf:160

Expected: API Gateway Stage should be associated with a Web Application Firewall

Checkmarx

KICS REPORT v2.1.1

EC2 Instance Has Public IP

Results 1

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description

EC2 Instance should not have a public IP address.

../../path/modules/module-1/main.tf:3592

Expected: 'associate_public_ip_address' should be defined and not null

EC2 Instance Monitoring Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

Description

EC2 Instance should have detailed monitoring enabled. With detailed monitoring enabled data is available in 1-minute periods

../../path/modules/module-1/main.tf:3592

Expected: 'monitoring' should be defined and not null

Public Lambda via API Gateway

Results 2

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Access Control

Description

Allowing to run lambda function using public API Gateway

../../path/modules/module-1/main.tf:148

Expected: 'source_arn' should not equal '/*/*'

../../path/modules/module-1/main.tf:3167

Expected: 'source_arn' should not equal '/*/*'

S3 Bucket Allows Public ACL

Results 3

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Access Control

Description

S3 bucket allows public ACL

../../path/modules/module-1/main.tf:3291

Expected: 'block_public_acls' should equal 'true'

../../path/modules/module-1/main.tf:3368

Expected: 'block_public_acls' should equal 'true'

../../path/modules/module-1/main.tf:3207

Checkmarx

KICS REPORT v2.1.1

Expected: 'block_public_acls' should equal 'true'

S3 Bucket Logging Disabled

Results 4

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

Description

Server Access Logging should be enabled on S3 Buckets so that all changes are logged and trackable

../../path/modules/module-1/main.tf:3277

Expected: 'logging' should be defined and not null

../../path/modules/module-1/main.tf:3354

Expected: 'logging' should be defined and not null

../../path/modules/module-1/main.tf:3194

Expected: 'logging' should be defined and not null

../../path/modules/module-1/main.tf:3412

Expected: 'logging' should be defined and not null

S3 Bucket Policy Accepts HTTP Requests

Results 2

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Encryption

Description

S3 Bucket policy should not accept HTTP Requests

../../path/modules/module-1/main.tf:3232

Expected: aws_s3_bucket_policy[allow_access_for_prod].policy should not accept HTTP Requests

../../path/modules/module-1/main.tf:3316

Expected: aws_s3_bucket_policy[allow_access_for_dev].policy should not accept HTTP Requests

S3 Bucket Without Ignore Public ACL

Results 3

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Insecure Configurations

Description

S3 bucket without ignore public ACL

../../path/modules/module-1/main.tf:3293

Expected: 'ignore_public_acls' should equal 'true'

../../path/modules/module-1/main.tf:3209

Expected: 'ignore_public_acls' should equal 'true'

../../path/modules/module-1/main.tf:3370

Expected: 'ignore_public_acls' should equal 'true'

S3 Bucket Without Restriction Of Public Bucket

Results 3

Checkmarx

KICS REPORT v2.1.1

Severity MEDIUM
Platform Terraform
Cwe
Category Insecure Configurations

Description

S3 bucket without restriction of public bucket

../../path/modules/module-1/main.tf:3371

Expected: 'restrict_public_buckets' should equal 'true'

../../path/modules/module-1/main.tf:3294

Expected: 'restrict_public_buckets' should equal 'true'

../../path/modules/module-1/main.tf:3210

Expected: 'restrict_public_buckets' should equal 'true'

S3 Bucket Without Versioning

Results **4**

Severity MEDIUM
Platform Terraform
Cwe
Category Backup

Description

S3 bucket should have versioning enabled

../../path/modules/module-1/main.tf:3354

Expected: 'versioning' should be true

../../path/modules/module-1/main.tf:3412

Expected: 'versioning' should be true

../../path/modules/module-1/main.tf:3194

Expected: 'versioning' should be true

../../path/modules/module-1/main.tf:3277

Expected: 'versioning' should be true

S3 Bucket with Unsecured CORS Rule

Results **1**

Severity MEDIUM
Platform Terraform
Cwe
Category Insecure Configurations

Description

If the CORS (Cross-Origin Resource Sharing) rule is defined in an S3 bucket, it should be secure

../../path/modules/module-1/main.tf:3250

Expected: 'cors_rule' to not allow all methods, all headers or several origins

Security Group With Unrestricted Access To SSH

Results **1**

Severity MEDIUM
Platform Terraform
Cwe
Category Networking and Firewall

Description

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

https://kics.io

Checkmarx

KICS REPORT v2.1.1

../../path/modules/module-1/main.tf:3468

Expected: aws_security_group[goat_sg] 'SSH' (Port:22) should not be public

VPC FlowLogs Disabled

Results 1

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Observability

Description

Every VPC resource should have an associated Flow Log

../../path/modules/module-1/main.tf:3424

Expected: aws_vpc[goat_vpc] should be the same as Flow Logs VPC id

VPC Subnet Assigns Public IP

Results 1

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description

VPC Subnet should not assign public IP

../../path/modules/module-1/main.tf:3442

Expected: aws_subnet[goat_subnet].map_public_ip_on_launch should be set to false or undefined

VPC Without Network Firewall

Results 1

Severity	MEDIUM
Platform	Terraform
Cwe	
Category	Networking and Firewall

Description

VPC should have a Network Firewall associated

../../path/modules/module-1/main.tf:3424

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

API Gateway Deployment Without API Gateway UsagePlan Associated

Results 1

Severity	LOW
Platform	Terraform
Cwe	
Category	Observability

Description

API Gateway Deployment should have API Gateway UsagePlan defined and associated.

../../path/modules/module-1/main.tf:2931

Expected: aws_api_gateway_deployment[apideploy_ba] has a 'aws_api_gateway_usage_plan' resource associated.

API Gateway Stage Without API Gateway UsagePlan Associated

Results 1

Severity	LOW

Checkmarx

KICS REPORT v2.1.1

Platform Terraform
Cwe
Category Resource Management

Description

API Gateway Stage should have API Gateway UsagePlan defined and associated.

../../path/modules/module-1/main.tf:160

Expected: aws_api_gateway_stage[api] has a 'aws_api_gateway_usage_plan' resource associated.

API Gateway With Invalid Compression

Results **2**

Severity LOW
Platform Terraform
Cwe
Category Encryption

Description

API Gateway should have valid compression, which means attribute 'minimum_compression_size' should be set and its value should be greater than -1 and smaller than 10485760.

../../path/modules/module-1/main.tf:172

Expected: Attribute 'minimum_compression_size' should be set and have a value greater than -1 and smaller than 10485760

../../path/modules/module-1/main.tf:66

Expected: Attribute 'minimum_compression_size' should be set and have a value greater than -1 and smaller than 10485760

API Gateway X-Ray Disabled

Results **1**

Severity LOW
Platform Terraform
Cwe
Category Observability

Description

API Gateway should have X-Ray Tracing enabled

../../path/modules/module-1/main.tf:160

Expected: 'aws_api_gateway_stage[api].xray_tracing_enabled' should be set

IAM Access Analyzer Not Enabled

Results **1**

Severity LOW
Platform Terraform
Cwe
Category Best Practices

Description

IAM Access Analyzer should be enabled and configured to continuously monitor resource permissions

../../path/modules/module-1/main.tf:23

Expected: 'aws_accessanalyzer_analyzer' should be set

Instance With No VPC

Results **1**

Severity LOW
Platform Terraform
Cwe
Category Insecure Configurations

Checkmarx

KICS REPORT v2.1.1

Description

EC2 Instances should be configured under a VPC network. AWS VPCs provide the controls to facilitate a formal process for approving and testing all network connections and changes to the firewall and router configurations.

../../path/modules/module-1/main.tf:3592

Expected: Attribute 'vpc_security_group_ids' should be defined and not null

Lambda Functions Without X-Ray Tracing

Results **2**

Severity	LOW
Platform	Terraform
Cwe	
Category	Observability

Description

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

../../path/modules/module-1/main.tf:23

Expected: aws_lambda_function[react_lambda_app].tracing_config should be defined and not null

../../path/modules/module-1/main.tf:3083

Expected: aws_lambda_function[lambda_ba_data].tracing_config should be defined and not null

Lambda IAM InvokeFunction Misconfigured

Results **2**

Severity	LOW
Platform	Terraform
Cwe	
Category	Best Practices

Description

Lambda permission may be misconfigured if the action field is not filled in by 'lambda:InvokeFunction'

../../path/modules/module-1/main.tf:3130

Expected: [lambda_data_policies].policy should be misconfigured

../../path/modules/module-1/main.tf:3520

Expected: [goat_inline_policy_2].policy should be misconfigured

DynamoDB Table Point In Time Recovery Disabled

Results **2**

Severity	INFO
Platform	Terraform
Cwe	
Category	Best Practices

Description

It's considered a best practice to have point in time recovery enabled for DynamoDB Table

../../path/modules/module-1/main.tf:3608

Expected: aws_dynamodb_table.point_in_time_recovery.enabled should be enabled

../../path/modules/module-1/main.tf:3620

Expected: aws_dynamodb_table.point_in_time_recovery.enabled should be enabled

EC2 Not EBS Optimized

Results **1**

Severity	INFO
Platform	Terraform

Checkmarx

KICS REPORT v2.1.1

Cwe
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

../../path/modules/module-1/main.tf:3592

Expected: 'ebs_optimized' should be set to true

Name Is Not Snake Case

Results **1**

Severity INFO
Platform Terraform
Cwe
Category Best Practices

Description

All names should follow snake case pattern.

../../path/modules/module-1/main.tf:172

Expected: All names should be on snake case pattern

Output Without Description

Results **1**

Severity INFO
Platform Terraform
Cwe
Category Best Practices

Description

All outputs should contain a valid description.

../../path/modules/module-1/main.tf:3708

Expected: 'description' should be defined and not null

Resource Not Using Tags

Results **24**

Severity INFO
Platform Terraform
Cwe
Category Best Practices

Description

AWS services resource tags are an essential part of managing components. As a best practice, the field 'tags' should have additional tags defined other than 'Name'

../../path/modules/module-1/main.tf:3488

Expected: aws_iam_role[{{goat_role}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3401

Expected: aws_s3_bucket_object[{{upload_temp_object_2}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3428

Expected: aws_vpc[{{goat_vpc}}].tags has additional tags defined other than 'Name'

../../path/modules/module-1/main.tf:3620

Expected: aws_dynamodb_table[{{posts_table}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3484

Expected: aws_iam_instance_profile[{{goat_iam_profile}}].tags should be defined and not null

Checkmarx

KICS REPORT v2.1.1

../../path/modules/module-1/main.tf:3443

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

../../path/modules/module-1/main.tf:66

Expected: aws_api_gateway_rest_api[{{api}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3128

Expected: aws_iam_policy[{{lambda_data_policies}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3264

Expected: aws_s3_bucket_object[{{upload_folder_prod}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3608

Expected: aws_dynamodb_table[{{users_table}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3341

Expected: aws_s3_bucket_object[{{upload_folder_dev_2}}].tags should be defined and not null

../../path/modules/module-1/main.tf:23

Expected: aws_lambda_function[{{react_lambda_app}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3332

Expected: aws_s3_bucket_object[{{upload_folder_dev}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3392

Expected: aws_s3_bucket_object[{{upload_temp_object}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3434

Expected: aws_internet_gateway[{{goat_gw}}].tags has additional tags defined other than 'Name'

../../path/modules/module-1/main.tf:3083

Expected: aws_lambda_function[{{lambda_ba_data}}].tags should be defined and not null

../../path/modules/module-1/main.tf:172

Expected: aws_api_gateway_rest_api[{{apiLambda_ba}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3598

Expected: aws_instance[{{goat_instance}}].tags has additional tags defined other than 'Name'

../../path/modules/module-1/main.tf:3448

Expected: aws_route_table[{{goat_rt}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3477

Expected: aws_security_group[{{goat_sg}}].tags has additional tags defined other than 'Name'

../../path/modules/module-1/main.tf:3518

Expected: aws_iam_policy[{{goat_inline_policy_2}}].tags should be defined and not null

../../path/modules/module-1/main.tf:160

Expected: aws_api_gateway_stage[{{api}}].tags should be defined and not null

../../path/modules/module-1/main.tf:35

Expected: aws_iam_role[{{blog_app_lambda}}].tags should be defined and not null

../../path/modules/module-1/main.tf:3102

Expected: aws_iam_role[{{blog_app_lambda_python}}].tags should be defined and not null

Security Group Rule Without Description

Results **2**

Severity	INFO
Platform	Terraform
Cwe	
Category	Best Practices

Description

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

https://kics.io

Checkmarx

KICS REPORT v2.1.1

../../path/modules/module-1/main.tf:3464

Expected: aws_security_group[{{goat_sg}}].ingress description should be defined and not null

../../path/modules/module-1/main.tf:3470

Expected: aws_security_group[{{goat_sg}}].egress description should be defined and not null

---