Checkmarx

KICS REPORT   development

CRITICAL	0	HIGH	2	MEDIUM	4	LOW	1	INFO	6	TOTAL	13

PLATFORMS   Terraform
START TIME   12:28:34, Jan 15 2025
END TIME   12:29:23, Jan 15 2025
SCANNED PATHS:
- /root/CaseStudyBatch-01/terraform

Sensitive Port Is Exposed To Entire Network

Results **1**

Severity	HIGH
Platform	Terraform
Cwe	200
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

../../CaseStudyBatch-01/terraform/vpc.tf:76

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

Unrestricted Security Group Ingress

Results **1**

Severity	HIGH
Platform	Terraform
Cwe	668
Category	Networking and Firewall

Description

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

../../CaseStudyBatch-01/terraform/vpc.tf:88

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

EC2 Instance Has Public IP

Results **1**

Severity	MEDIUM
Platform	Terraform
Cwe	200
Category	Networking and Firewall

Description

EC2 Instance should not have a public IP address.

../../CaseStudyBatch-01/terraform/vpc.tf:114

Expected: 'associate_public_ip_address' should be set to false

HTTP Port Open To Internet

Results **1**

Severity	MEDIUM
Platform	Terraform
Cwe	319
Category	Networking and Firewall

Description

The HTTP port is open to the internet in a Security Group

../../CaseStudyBatch-01/terraform/vpc.tf:71

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

https://kics.io

Checkmarx

| KICS REPORT | development |

🛡 VPC FlowLogs Disabled

Results   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	778
Category	Observability

Description

Every VPC resource should have an associated Flow Log

../../CaseStudyBatch-01/terraform/vpc.tf:12

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

🛡 VPC Without Network Firewall

Results   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	311
Category	Networking and Firewall

Description

VPC should have a Network Firewall associated

../../CaseStudyBatch-01/terraform/vpc.tf:12

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

🛡 IAM Access Analyzer Not Enabled

Results   **1**

Severity	LOW
Platform	Terraform
Cwe	710
Category	Best Practices

Description

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

../../CaseStudyBatch-01/terraform/vpc.tf:12

Expected: 'aws_accessanalyzer_analyzer' should be set

🛡 EC2 Not EBS Optimized

Results   **1**

Severity	INFO
Platform	Terraform
Cwe	710
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

../../CaseStudyBatch-01/terraform/vpc.tf:106

Expected: 'ebs_optimized' should be set to true

🛡 Resource Not Using Tags

Results   **1**

Severity	INFO
Platform	Terraform
Cwe	665

| **KICS REPORT** | **development** |

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'

../../CaseStudyBatch-01/terraform/vpc.tf:52

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

🛡 **Security Group Rule Without Description**   **Results**   **3**

Severity	INFO
Platform	Terraform
Cwe	710
Category	Best Practices

Description

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

../../CaseStudyBatch-01/terraform/vpc.tf:76

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

../../CaseStudyBatch-01/terraform/vpc.tf:92

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

../../CaseStudyBatch-01/terraform/vpc.tf:84

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

🛡 **Security Group Without Description**   **Results**   **1**

Severity	INFO
Platform	Terraform
Cwe	710
Category	Best Practices

Description

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

../../CaseStudyBatch-01/terraform/vpc.tf:71

Expected: aws_security_group[{{acn_sg}}] description should be defined and not null