

Checkmar



A New Attack Vector

Infrastructure as Code



A B O U T M E



R u s t y S i d e s

DIRECTOR OF SALES ENGINEERING

- Security Evangelist
- Software Developer prior to AppSec
- Strong Believer in spreading Awareness for Software Security



Checkmarx Recognized by Gartner

5 Years in a Row

Checkmarx is positioned by Gartner® as a Leader in the April 2022 Magic Quadrant¹ for Application Security Testing.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Checkmarx. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner

Source: Gartner, Magic Quadrant for Application Security Testing by Dale Gardner, Mark Horvath, Dionisio Zumerle, 18 April 2022

Figure 1: Magic Quadrant for Application Security Testing

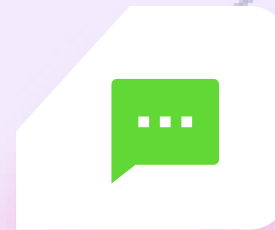
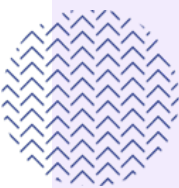


As of April 2022 © Gartner, Inc

Source: Gartner (April 2022)



EVERYTHING IS CODE



Everything >>>>>

CAN BE TREATED LIKE
APPLICATION CODE SUCH THAT
WE CAN FOLLOW THE SAME
SOFTWARE DEVELOPMENT
LIFECYCLE PRACTICES



IT'S ALL "CODE"

0 1

Application
Configuration

0 2

Operating System
and Host
Configuration

0 3

Cloud Resources

0 4

Network Elements



0 5

Firewalls

0 6

Load Balancers

0 7

Security Groups

0 8

IoT Devices



THE BENEFITS OF CODE



Automation



GitOps



Code
Review



Testing



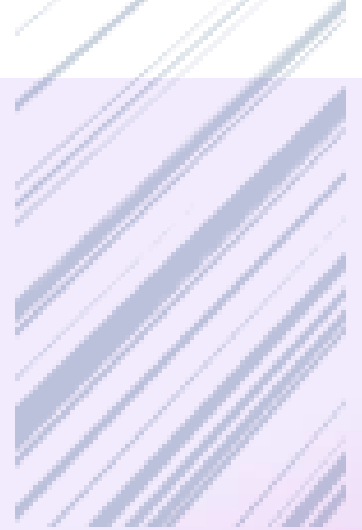
Version
Control



Reversibility



I n f r a s t r u c t u r e a s c o d e (I a C)



```
age;  
OM marks WHERE subject_ID=" +  
atasetsWithSubject) {  
atasetsWithSubject.length > 0) {  
ctAverage = 0;  
etsWithSubjectLength = dataset  
etsWithSubject.forEach((dataset  
bjectAverage += parseFloat(da  
tAverage =  
bjectAverage / dataset
```

IS THE PROCESS OF **MANAGING
AND PROVISIONING SOFTWARE**
THROUGH MACHINE-READABLE
DEFINITION FILES, RATHER THAN
PHYSICAL HARDWARE
CONFIGURATION OR INTERACTIVE
CONFIGURATION TOOLS



WHAT IS INFRASTRUCTURE-AS-CODE (IAC)



IaC automates the manual tasks usually associated with computing infrastructure configuration and implementation.



IaC
allows
you to:

01

SPEED UP

Speed up configuration and implementation of new computing infrastructure

02

REDUCE THE COST

Reduce the cost and resource needed to scale and manage large infrastructure

03

ELIMINATE THE INCONSISTEN- CIES

Eliminate the inconsistencies that inevitably occur when multiple individuals manually configure new equipment or applications.





INFRASTRUCTURE AT THE SPEED OF DEVOPS

Moving to cloud-based infrastructure opens doors to building and managing infrastructure in completely new ways:

0 1

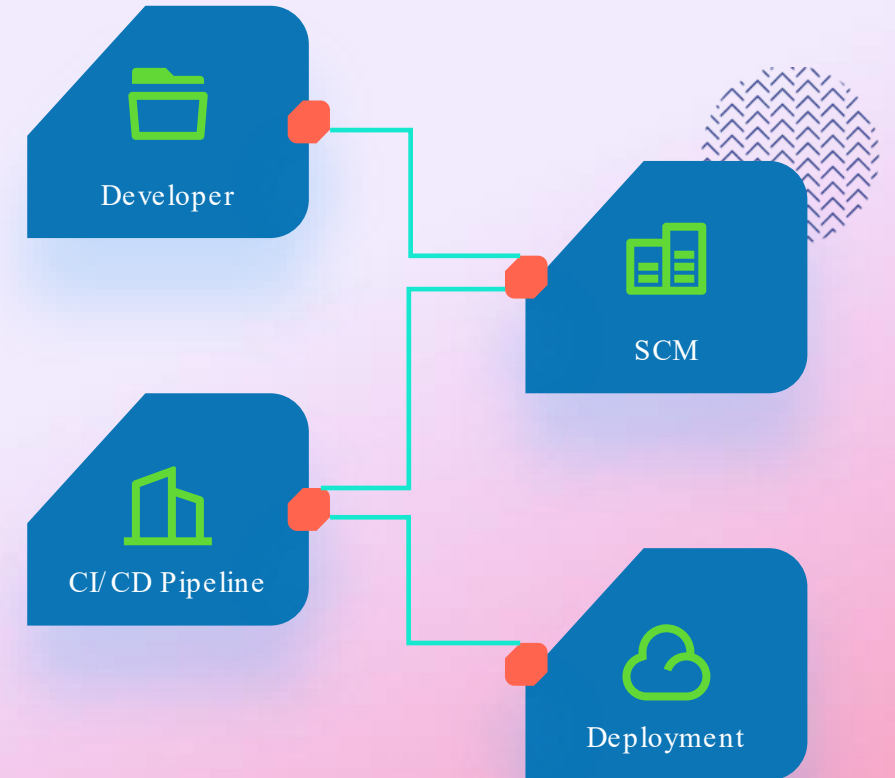
Infrastructure can be provisioned in seconds

0 2

Scale can be achieved without capacity planning

0 3

API-driven cloud infra allows us interact with it via code





SO, WHAT'S THE
PROBLEM?



I A C S E C U R I T Y I S A C O N C E R N

2 0 0 , 0 0 0

IaC Templates

4 8 %

of AWS S3 buckets do
not have server-side
encryption enabled

4 2 %

CloudFormation config files
contained at least one
insecure configuration

5 5 %

of cloud user-configured
S3 buckets do not have
logging enabled

Source: <https://start.paloaltonetworks.com/unit-42-cloud-threat-report>



An SSRF, privileged AWS keys and the Capital One breach



Riyaz Walikar

Follow

Aug 4, 2019 · 9 min read



This post attempts to explain the technical side of how the Capital One breach occurred, the impact of the breach and what you can do as a user of cloud services to prevent this from happening to you.

Updated 3rd December 2019 — Please note: AWS released an additional security defences against the attack mentioned in this blog post. While the methods described here will work with the legacy version of Instance Metadata Service (IMDSv1), they will be thwarted by IMDSv2. Read our extensive blog post on how to utilise AWS EC2 IMDSv2 and add the additional defences for your EC2 machines

02 What We Can Learn from the Capital One Hack

AUG 19

On Monday, a former **Amazon** employee was arrested and charged with **stealing more than 100 million consumer applications for credit from Capital One**. Since then, many have speculated the breach was perhaps the result of a previously unknown “zero-day” flaw, or an “insider” attack in which the accused took advantage of access surreptitiously obtained from her former employer. But new information indicates the methods she deployed have been well understood for years.



SECURITY RISKS IN IAC IMPLEMENTATIONS

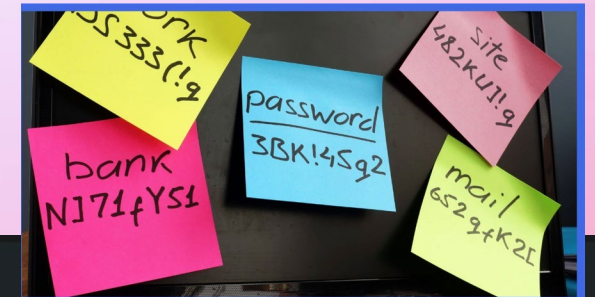
- Vulnerabilities in IaC can serve as a thread entry point to the core infrastructure
- Misconfigured IaC templates can expose sensitive data



SECRETS STORAGE

Keep it secret, Keep it safe

- Storage of secrets is necessary for connecting to managed infrastructure.
- Storing such data inside source code management (SCM) systems or plain text files is dangerous and irresponsible.
- Bots scrape public SCM sites like Github looking for secrets to exploit and compromise



```
/*public static void main(String[] args) {  
    // Endpoint以Region: 华东1为例, 其他Region请按实际情况填写  
    String endpoint = "https://datahub.cn-shanghai-shga-d01.dh.alicloud.ga.sh";  
    String accessId = "0iWV0NCs805VuAAu";  
    String accessKey = "iEwlgpCnXDwT93YMVDb2G60my9ne81";  
    String projectName = "sjc_rwzx";  
    String topicName = "task_center_platform_request";  
    RecordSchema schema = new RecordSchema();
```

USER PRIVILEGES

Least privilege

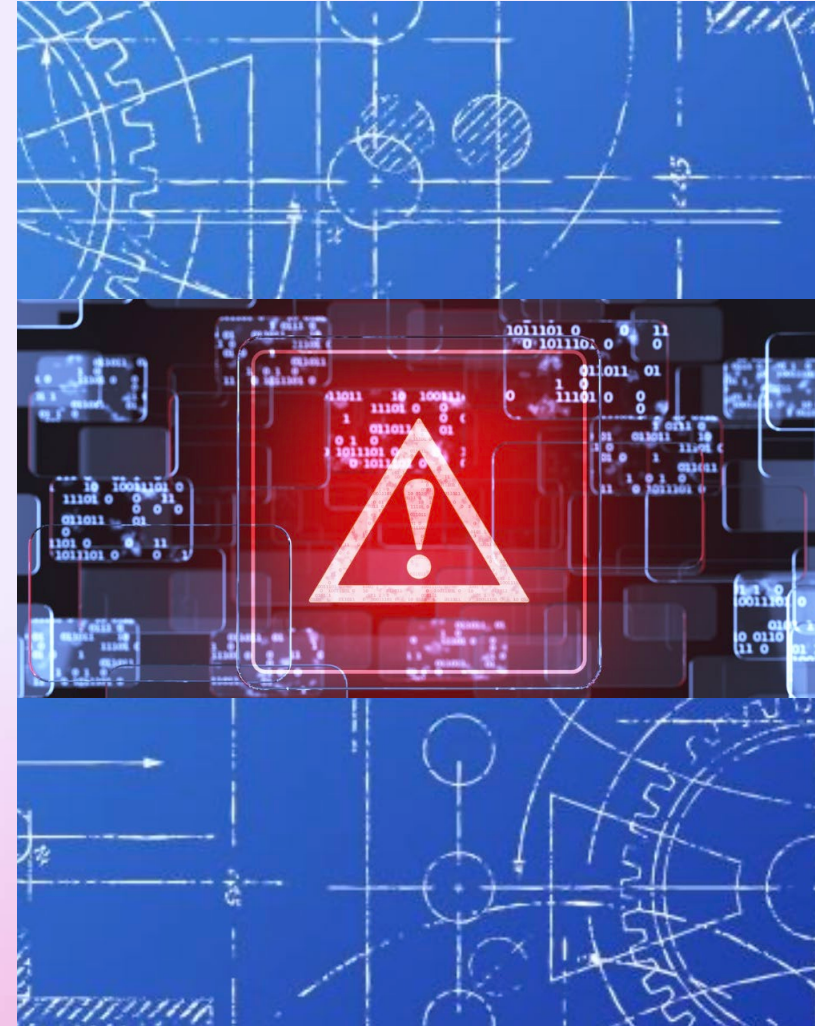
- Application deployment is unlikely to require root privileges on the target machine
- Least privilege may be more challenging but mitigates the risk of compromise



I A C T E M P L A T E S

Do you trust the source?

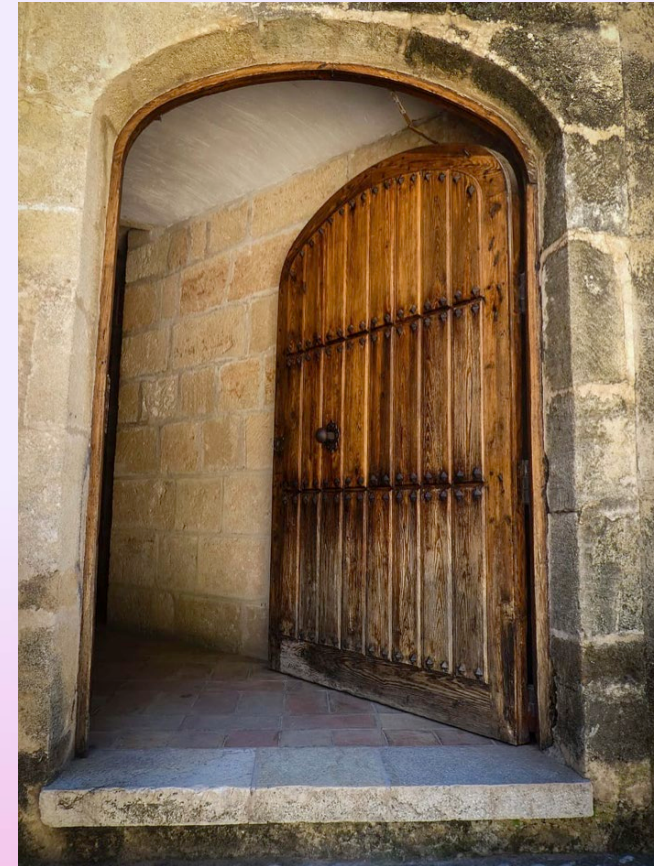
- IaC Templates can have vulnerabilities and insecure default configurations that could lead to data exposure
- IaC Templates can unintentionally use OS or container images from untrusted sources



NETWORK EXPOSURES

New platforms, New problems

- Insecure IaC configurations can expand the attack surface
- Open Security Groups
- Public SSH Access





EXAMPLE OF IAC AWS CLOUDFORMATION



CloudFormation



```
ElasticBeanstalkSample.template
1 {
2   "AWSTemplateFormatVersion" : "2010-09-09",
3
4   "Description" : "AWS CloudFormation Sample Template ElasticBeanstalkSample: Configure and
5
6   "Parameters" : {
7     "KeyName" : {
8       "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the AWS Elast
9       "Type" : "String"
10    }
11  },
12
13  "Resources" : {
14    "sampleApplication" : {
15      "Type" : "AWS::ElasticBeanstalk::Application",
16      "Properties" : {
17        "Description" : "AWS Elastic Beanstalk Sample Application",
18        "ApplicationVersions" : [{
19          "VersionLabel" : "Initial Version",
20          "Description" : "Version 1.0",
21          "SourceBundle" : {
22            "S3Bucket" : { "Fn::Join" : ["-", ["elasticbeanstalk-samples", { "Ref" : "AWS::R
23            "S3Key" : "elasticbeanstalk-sampleapp.war"
24          }
25        }
26      },
27      "ConfigurationTemplates" : [{
28        "TemplateName" : "DefaultConfiguration",
29        "Description" : "Default Configuration Version 1.0 - with SSH access",
30        "SolutionStackName" : "64bit Amazon Linux running Tomcat 7",
```

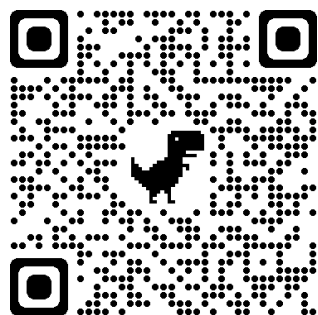


Keeping Infrastructure as Code Secure

kicks.io



KICS IS OPEN-SOURCE



Public GitHub
repository

([https://github.com/
Checkmarx/kics](https://github.com/Checkmarx/kics))



Live chat
with Gitter

([https://gitter.im/kics-
io/community](https://gitter.im/kics-io/community))



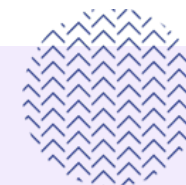
Public
website

(<https://kics.io/>)



Managed
completely
from GitHub

(Issues / Projects)



S U P P O R T E D P L A T F O R M S



Terraform

Kubernetes

Docker

AWS CloudFormation

Ansible

Helm

Google Deployment

Manager

AWS SAM

Microsoft ARM

OpenAPI 3.0



KICS : SECURITY POLICIES

- ▶ Access Control
- ▶ Availability
- ▶ Backup
- ▶ Best Practices
- ▶ Build Process
- ▶ Encryption
- ▶ Insecure configurations
- ▶ Insecure defaults
- ▶ Networking and Firewall
- ▶ Observability
- ▶ Resource management
- ▶ Secret management
- ▶ Supply-Chain

Supports top
Infrastructure-as-
Code tools with over
2000 security
policies

KICS : VULNERABILITY EXAMPLE

```
resource "azurerm_network_security_rule" "positive4" {  
  name           = "example"  
  priority       = 100  
  direction     = "Inbound"  
  access        = "Allow"  
  protocol      = "TCP"  
  source_port_range = "*"  
  destination_port_range = "22"  
  source_address_prefix = "0.0.0.0"  
  destination_address_prefix = "*"  
  resource_group_name   = azurerm_resource_group.example.name  
  network_security_group_name = azurerm_network_security_group.example.name  
}
```

0 1

Terraform for Azure

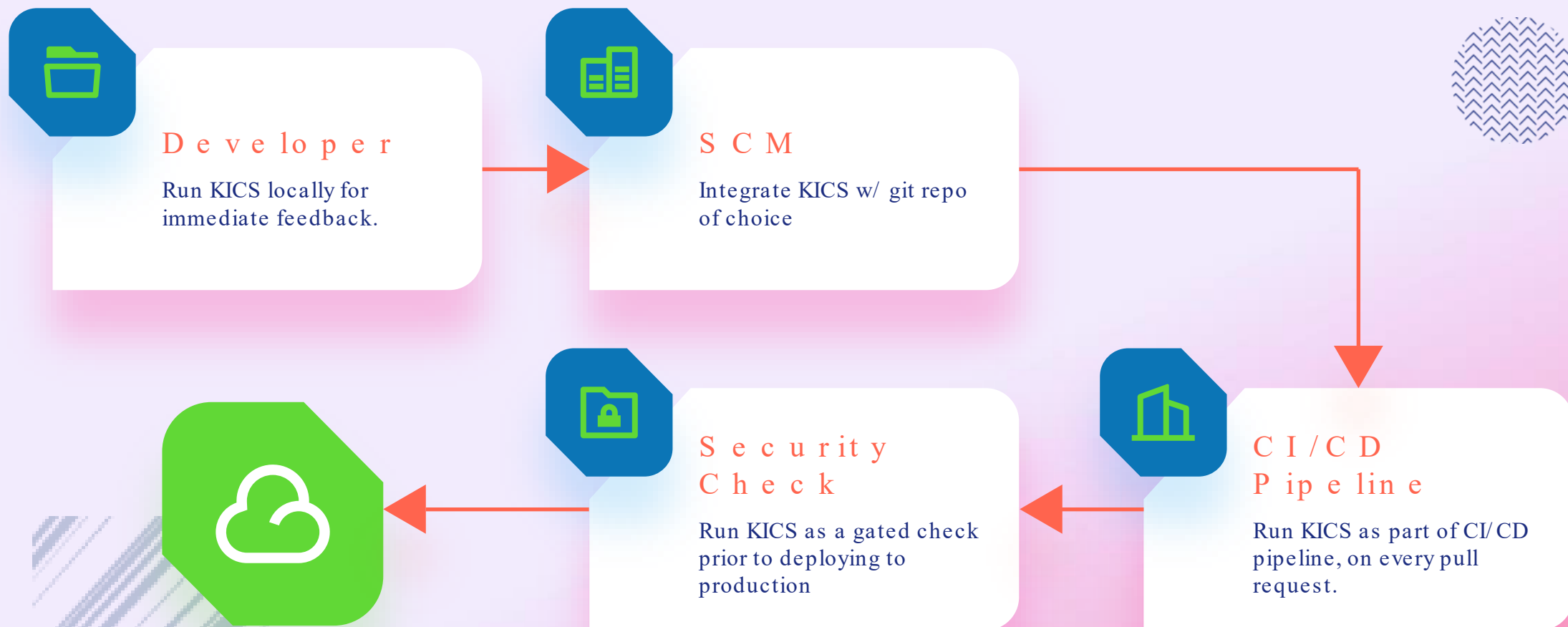
0 2

Access policy for a resource

0 3

SSH port 22 is left open leaving the possibility of unauthorized access, ports scanning attacks and remote take-over of your infrastructure

KICS : INTEGRATION FLOW DIAGRAM





LIVE DEMO



keeping infrastructure as code secure is an
open source solution for static code analysis
of Infrastructure as Code.

<https://kics.io>



Scan your IaC

Get results immediately

Supported file types: zip .tf .json .yaml .yml .dockerfile (max size 4MB)

 Or drag & drop, or [browse](#) file

☐ I agree to the [terms of service](#)

START YOUR SCAN

KICS finds security vulnerabilities, compliance issues, and infrastructure misconfigurations in following Infrastructure as Code solutions: Terraform, Kubernetes, Docker, AWS CloudFormation, Ansible. 1900+ queries are available.

Complete

KICS finds security vulnerabilities, compliance issues, and infrastructure misconfigurations in following Infrastructure as Code solutions: Terraform, Kubernetes, Docker, AWS CloudFormation, Ansible. 1900+ queries are available.

KICS is easy to install and run, easy to understand results, and easy to integrate into CI.

Open Source

KICS is open and will always stay such. Both the scanning engine and the security queries are clear and open for the software development community.

Extensible

From day one KICS is built for extensibility.

First, it includes over 1900 fully customizable and adjustable heuristics rules, called queries. These can be easily edited, extended, and added. Second, its robust but yet simple architecture allows quick addition of support for new Infrastructure as Code solutions.



KICS REPORT

v1.5.3

HIGH	99	MEDIUM	61	LOW	21	INFO	62	TOTAL	243
------	----	--------	----	-----	----	------	----	-------	-----

PLATFORMS Terraform, Dockerfile, Common

START TIME 19:44:19, Jul 14 2022

END TIME 19:44:59, Jul 14 2022

SCANNED PATHS:

- git::https://github.com/bridgecrewio/terragoat.git



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

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/sql.tf:9

Expected: A 'azurem_sql_active_directory_administrator' is defined for 'azurem_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

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:43

Expected: 'azurem_app_service[app-service2].identity' is defined and not null

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:22

Expected: 'azurem_app_service[app-service1].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

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:29

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



```
efriese@mint-clean:~/tmp/kics/bin$ ./kics scan -p ../../terragoat/ --report-formats json
```

```
.0MO.
OMMMx
;NMx;

...
...
...
WMMMd      cWMMMO.  KMMMO      ;xKWMMMN0c.      ,xXMMMMWxkc.
WMMMd      .0MMMN:  KMMMO      :XMMMMMMMMMMMMWl  xMMMMMMWMMMMMMl
WMMMd      lWMMMO.  KMMMO      xMMMMKc...'lXmk  ,MMMMx      ;dXx
WMMMd      .0MMMX;  KMMMO      cMMMMd      '      'MMMMNl'
WMMMMNMMMMMl      KMMMO      0MMMN      oMMMMMMMMXkl.
WMMMMMMMMMMMo      KMMMO      0MMMX      .ckKWMMMMMMO.
WMMMMWokMMMMk      KMMMO      oMMMMc      .      :0MMMMO
WMMMK.      dMMMMO.  KMMMO      KMMMMx'      ,kNc      :W0c.      .NMMMX
WMMMd      cWMMMX.  KMMMO      kMMMMMMWXNMMMMMMd .WMMMMWKO0NMMMMl
WMMMd      ,NMMMN,  KMMMO      'xNMMMMMMMMNx,  .l0WMMMMMMMMwk,
xkkk:      ,kkkkx  okkk      ;xKKX;      ;d0KKkc
```

Scanning with Keeping Infrastructure as Code Secure snapshot-7e8b65d9

Preparing Scan Assets: Done

Executing queries: [-----] 100.00%

Files scanned: 51

Parsed files: 51

Queries loaded: 1311

Queries failed to execute: 0

Variable Without Type, Severity: INFO, Results: 7

Description: All variables should contain a valid type.

Platform: Terraform

[1]: ../../terragoat/terraform/aws/consts.tf:20

019:

020: variable "profile" {

021: default = "default"

[2]: ../../terragoat/terraform/gcp/variables.tf:16

015:

🛡️ Web App Accepting Traffic Other Than HTTPS | AppSec HD Assistance

🛡️ High ▾

📄 To Verify ▾

app_service.tf

```
15   git_modifiers    = "nimrodkor"
16   git_org          = "bridgecrewio"
17   git_repo         = "terragoat"
18   yor_trace        = "6611bf45-fd5b-467e-b119-d533cd7539b8"
19 }
20 }
21
22 resource azurerm_app_service "app-service1" {
23   app_service_plan_id = azurerm_app_service_plan.example.id
24   location            = var.location
25   name               = "terragoat-app-service-${var.environment}${random_integer.rnd_int.result}"
26   resource_group_name = azurerm_resource_group.example.name
27   https_only          = false
28   site_config {
29     min_tls_version = "1.1"
30   }
31   tags = {
32     git_commit    = "81738b80d571fa3034633690d13ffb460e1e7dea"
33     git_file      = "terraform/azure/app_service.tf"
34     git_last_modified_at = "2020-06-19 21:14:50"
35     git_last_modified_by = "Adin.Ermie@outlook.com"
36     git_modifiers  = "Adin.Ermie/nimrodkor"
37     git_org        = "bridgecrewio"
38     git_repo       = "terragoat"
39     yor_trace      = "13be096d-c599-46e5-bf54-51c6e9732858"
```

Description

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

📄 File

/terraform/azure/app_service.tf

❗ Value

'azurerm_app_service[app-service1].https_only' is not set to true

✅ Expected Value

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

243 Vulnerabilities

Primary Grouping: Platform ▾

Secondary Grouping: Severity ▾

⚙️ Add filter

📁 Terraform (226)

📁 🛡️ High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Web App Accepting Traffic Other...	/terraform/azure/app_service.tf	To Verify	'azurerm_app_service[app-servic...	'azurerm_app_service[app-servic...	Inco...	Insecure Configurations

🛡️ Web App Accepting Traffic Other Than HTTPS | AppSec HD Assistance

app_service.tf

```

15   git_modifiers    = "nimrodkor"
16   git_org           = "bridgecrewio"
17   git_repo          = "terragoat"
18   yor_trace         = "6611bf45-fd5b-467e-b119-d533cd7539b8"
19 }
20 }
21
22 resource azurerm_app_service "app-service1" {
23   app_service_plan_id = azurerm_app_service_plan.example.id
24   location             = var.location
25   name                 = "terragoat-app-service-${var.environment}${random_integer.rnd_int.result}"
26   resource_group_name = azurerm_resource_group.example.name
27   https_only           = false
28   site_config {
29     min_tls_version = "1.1"
30   }
31   tags = {
32     git_commit    = "81738b80d571fa3034633690d13ffb460e1e7dea"
33     git_file       = "terraform/azure/app_service.tf"
34     git_last_modified_at = "2020-06-19 21:14:50"
35     git_last_modified_by = "Adin.Ermie@outlook.com"
36     git_modifiers    = "Adin.Ermie/nimrodkor"
37     git_org          = "bridgecrewio"
38     git_repo         = "terragoat"
39     yor_trace        = "13be096d-c599-46e5-bf54-51c6e9732858"

```

High
Medium
Low
Info

Description

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

📄 File

/terraform/azure/app_service.tf

🚫 Value

'azurerm_app_service[app-service1].https_only' is not set to true

✅ Expected Value

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

243 Vulnerabilities

Primary Grouping: Platform ▾

Secondary Grouping: Severity ▾

⚙️ Add filter

📁 Terraform (226)

📁 🛡️ High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Web App Accepting Traffic Other...	/terraform/azure/app_service.tf	To Verify	'azurerm_app_service[app-servic...	'azurerm_app_service[app-servic...	Inco...	Insecure Configurations

Web App Accepting Traffic Other Than HTTPS | AppSec HD Assistance

High To Verify

app_service.tf

```
15   git_modifiers    = "nimrodkor"
16   git_org           = "bridgecrewio"
17   git_repo          = "terragoat"
18   yor_trace         = "6611bf45-fd5b-467e-b119-d533cd7539b8"
19 }
20 }
21
22 resource azurerm_app_service "app-service1" {
23   app_service_plan_id = azurerm_app_service_plan.example.id
24   location             = var.location
25   name                 = "terragoat-app-service-${var.environment}${random_integer.rnd_int.result}"
26   resource_group_name = azurerm_resource_group.example.name
27   https_only           = false
28   site_config {
29     min_tls_version = "1.1"
30   }
31   tags = {
32     git_commit    = "81738b80d571fa3034633690d13ffb460e1e7dea"
33     git_file      = "terraform/azure/app_service.tf"
34     git_last_modified_at = "2020-06-19 21:14:50"
35     git_last_modified_by = "Adin.Ermie@outlook.com"
36     git_modifiers    = "Adin.Ermie/nimrodkor"
37     git_org          = "bridgecrewio"
38     git_repo         = "terragoat"
39     yor_trace        = "13be096d-c599-46e5-bf54-51c6e9732858"
```

Description

Web app should only accept HTTPS Web App Service.

File

/terraform/azure/app_service.tf

Value

'azurerm_app_service[app-service1].https_only' is not set to true

Expected Value

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

Not Exploitable
Proposed Not Exploitable
Confirmed
Urgent

243 Vulnerabilities

Primary Grouping: Platform

Secondary Grouping: Severity

Add filter

Terraform (226)

High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Web App Accepting Traffic Other...	/terraform/azure/app_service.tf	To Verify	'azurerm_app_service[app-servic...	'azurerm_app_service[app-servic...	Inco...	Insecure Configurations



Security Group With Unrestricted Access To SSH | AppSec HD Assistance

High

To Verify

ec2.tf

```
75 }
76
77 resource "aws_security_group" "web-node" {
78   # security group is open to the world in SSH port
79   name       = "${local.resource_prefix.value}-sg"
80   description = "${local.resource_prefix.value} Security Group"
81   vpc_id     = aws_vpc.web_vpc.id
82
83   ingress {
84     from_port = 80
85     to_port   = 80
86     protocol  = "tcp"
87     cidr_blocks = [
88       "0.0.0.0/0"
89     ]
90   }
91   ingress {
92     from_port = 22
93     to_port   = 22
94     protocol  = "tcp"
95     cidr_blocks = [
96       "0.0.0.0/0"
97     ]
98   }
99   egress {
100    from_port = 0
101    to_port   = 0
```

Description

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

File

/terraform/aws/ec2.tf

Value

aws_security_group[web-node] 'SSH' (Port:22) is public

Expected Value

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

243 Vulnerabilities

Primary Grouping: Platform

Secondary Grouping: Severity

Add filter

Terraform (226)

High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Stackdriver Logging Disabled	/terraform/gcp/gke.tf	To Verify	Attribute 'logging_service' is 'none'	Attribute 'logging_service' is not '...	Inco...	Observability
☐	Recurrent	Security Group With Unrestricted...	/terraform/aws/ec2.tf	To Verify	aws_security_group[web-node] '...	aws_security_group[web-node] '...	Inco...	Networking And Firewall





SQL DB Instance Is Publicly Accessible | AppSec HD Assistance

High

To Verify

big_data.tf

```
1 resource "google_sql_database_instance" "master_instance" {
2   name           = "terragoat-${var.environment}-master"
3   database_version = "POSTGRES_11"
4   region         = var.region
5
6   settings {
7     tier = "db-f1-micro"
8     ip_configuration {
9       ipv4_enabled = true
10      authorized_networks {
11        name = "www"
12        value = "0.0.0.0/0"
13      }
14    }
15    backup_configuration {
16      enabled = false
17    }
18  }
19 }
20
21 resource "google_bigquery_dataset" "dataset" {
22   dataset_id = "terragoat_${var.environment}_dataset"
23   access {
24     special_group = "allAuthenticatedUsers"
25     role          = "READER"
26   }
27 }
```

Description

Check if any Cloud SQL instances are publicly accessible.

File

/terraform/gcp/big_data.tf

Value

'authorized_network' address is not restricted:
'0.0.0.0/0'

Expected Value

'authorized_network' address is trusted

243 Vulnerabilities

Primary Grouping: Platform

Secondary Grouping: Severity

Add filter

Terraform (226)

High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Stackdriver Logging Disabled	/terraform/gcp/gke.tf	To Verify	Attribute 'logging_service' is 'none'	Attribute 'logging_service' is not '...	Inco...	Observability





SQL DB Instance Backup Disabled | AppSec HD Assistance

High

To Verify

big_data.tf

```
4 region = var.region
5
6 settings {
7   tier = "db-f1-micro"
8   ip_configuration {
9     ipv4_enabled = true
10    authorized_networks {
11      name = "www"
12      value = "0.0.0.0/0"
13    }
14  }
15  backup_configuration {
16    enabled = false
17  }
18 }
19 }
20
21 resource "google_bigquery_dataset" "dataset" {
22   dataset_id = "terragoat_${var.environment}_dataset"
23   access {
24     special_group = "allAuthenticatedUsers"
25     role = "READER"
26   }
27   labels = {
28     git_commit = "2bdc0871a5f4505be58244029cc6485d45d7bb8e"
```

Description

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

File

/terraform/gcp/big_data.tf

Value

settings.backup_configuration.enabled is false

Expected Value

settings.backup_configuration.enabled is true

243 Vulnerabilities

Primary Grouping: Platform

Secondary Grouping: Severity

Add filter

Terraform (226)

High (83)

☐	Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
☐	Recurrent	Stackdriver Logging Disabled	/terraform/gcp/gke.tf	To Verify	Attribute 'logging_service' is 'none'	Attribute 'logging_service' is not '...	Inco...	Observability





S3 Bucket ACL Allows Read Or Write to All Users

AppSec HD Assistance

High

To Verify

s3.tf

```
1 resource "aws_s3_bucket" "data" {
2   # bucket is public
3   # bucket is not encrypted
4   # bucket does not have access logs
5   # bucket does not have versioning
6   bucket      = "${local.resource_prefix.value}-data"
7   acl         = "public-read"
8   force_destroy = true
9   tags = merge({
10    Name      = "${local.resource_prefix.value}-data"
11    Environment = local.resource_prefix.value
12  }, {
13    git_commit      = "4d57f83ca4d3a78a44fb36d1dcf0d23983fa44f5"
14    git_file        = "terraform/aws/s3.tf"
15    git_last_modified_at = "2022-05-18 07:08:06"
16    git_last_modified_by = "nimrod@bridgecrew.io"
17    git_modifiers    = "nimrod/nimrodkor"
18    git_org          = "bridgecrewio"
19    git_repo         = "terragoat"
20    yor_trace        = "0874007d-903a-4b4c-945f-c9c233e13243"
21  })
22 }
23
24 resource "aws_s3_bucket_object" "data_object" {
25   bucket = aws_s3_bucket.data.id
```

Description

S3 bucket with public READ/WRITE access

File

/terraform/aws/s3.tf

Value

'acl' is equal 'public-read'

Expected Value

'acl' is equal 'private'

243 Vulnerabilities

Primary Grouping: Platform

Secondary Grouping: Severity

Add filter

Terraform (226)

High (83)

Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
Recurrent	S3 Bucket Without Enabled MFA ...	/terraform/aws/ec2.tf	To Verify	aws_s3_bucket[flowbucket].versi...	aws_s3_bucket[flowbucket].versi...	Mis...	Insecure Configurations





Keeping Infrastructure as Code Secure

kicks.io



T h a n k y o u !