Checkmarx
The world runs on code. We secure it.

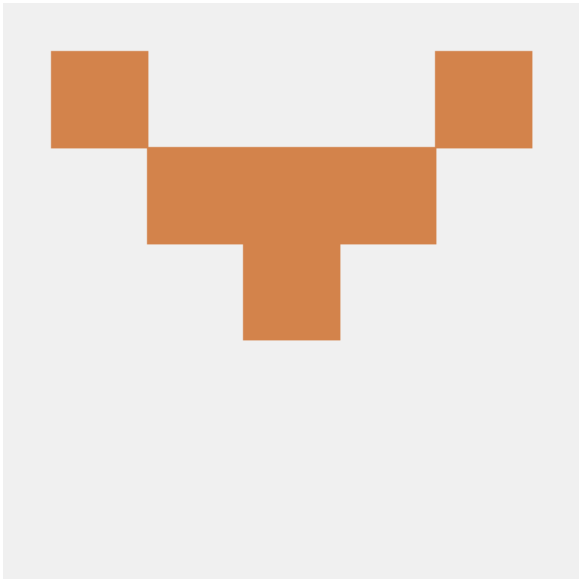
KICS

Community Meeting

2022.10.06

Meet the KICS team

KICS contributors (2+ commits)



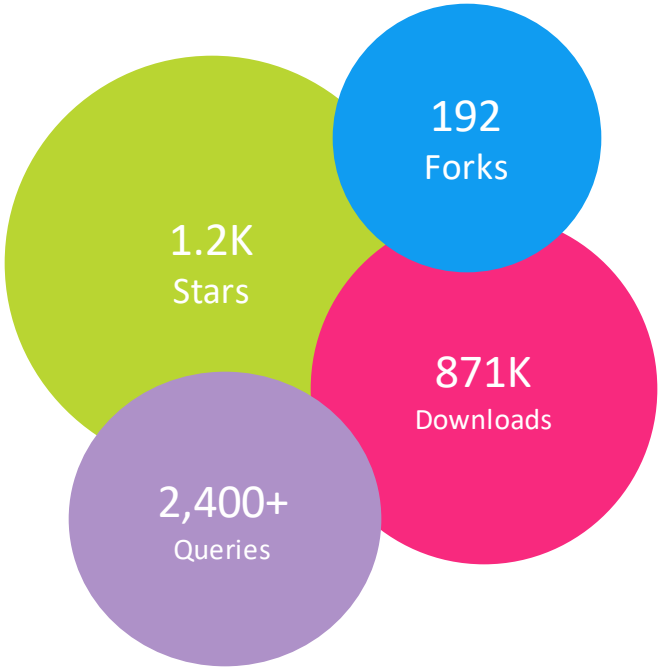

Community meetings

- **Bi-weekly meeting of the community & the KICS team.**
- **Meeting in mid sprint to:**
  - **Conclude the previous sprint & release**
  - **Talk about upcoming release & following sprint**
  - **Hear you, the community, on what interests you & what do you want to do / help with.**

KICS 1.6 contributors:
@sluetze @tomk-orca @liorj-orca @konstruktoid @VladMasarik @jycamier @Churro @patrickpichler @JoaoDanielRufino

KICS 1.5 contributors:
@rndmh3ro @Churro @jplanckeel @AlexEndris @liorj-orca @lipeavelar @roi-orca @LupovichRan @ramprasathasokan @nv35 @konstruktoid @jaevans @roock @tspearconquest @jycamier @floh96 @rams3sh @gafnit-lightspin

KICS Community Updates – 2022-10-06



KICS 1.6.1 was released

KICS Github Action upgarded to 1.6 (with KICS 1.6.0) - Github Action 1.5 runs with KICS 1.5.15

Community PR Merged (for KICS 1.6.2)

+ fix(query): terraform/aws/iam_access_key_is_exposed #5846 - @jycamier
+ fix(query): correct GCP KMS crypto key rotation period queries + descriptions #5863 - @Churro
+ feat(query): reduce NET_RAW capability not being dropped severity to MEDIUM #5900 - @patrickpichler
+ feat(query): drop Configuration Aggregator to All Regions Disabled Security severity to MEDIUM #5901 - @patrickpichler
+ fix(query): fix false positive in aws_instance #5903 - @patrickpichler
+ fix(query): fix false positive for rds backup_retention_period not set #5902 - @patrickpichler
+ fix(query): remove redundant and flawed GCP KMS key rotation query #5864 - @Churro

Community PR Pending (for later version)

+ change to use working directory when looking for `kics.config` #5319 - @lipeavelar
+ fix(query): cover additional deprecated API versions in k8s rule #5867 - @Churro
+ fix(query): S3 Bucket Without Restriction Of Public Bucket Security Query False Positive Result #5911 - @JoaoDanielRufino

Release

1.6.0 - 2022.09.14

- **Highlights**

- Support Crossplane, Knative, Pulumi and Serverless technologies.
- KICS Auto-Remediation feature for terraform files (details).
- Dynamic scanning of Kubernetes clusters (details).
- .gitignore processing by default.
- -t flag behavior changed for consistency purposes.
- Masking secrets on results when KICS finds them.

v1.6.0 Latest

New features and improvements

feat(knative&crossplane): add support to knative and crossplane (#5634)
feat(report): hide secrets in report results (#5504)
feat(scan): consider .gitignore to automatically exclude paths by default (#5506)
feat(pulumi): add support to Pulumi yaml parsing (#5648)
queries(pulumi): add pulumi gcp security queries (#5654)
queries(pulumi): add pulumi aws security queries (#5653)
queries(pulumi): add pulumi azure security queries (#5658)
feat(serverlessfw): add support to serverless fw yml file parsing (#5670)
feat(knative): add knative security query and k8's pod queries interoperability (#5692)
feat(queires): add serverless framework queries (#5679)
feat(serverless): initial cloudformation security queries refactoring (#5697)
feat(engine): Kubernetes API support for runtime k8s clusters scan (#5651)

Bug fixes

fix(resolver): exclude resolve path call for the same path reference (#5511) (#5514)

Dependency updates bumps

build(deps): bump github.com/zclconf/go-cty from 1.10.0 to 1.11.0
build(deps): bump github.com/aws/aws-sdk-go from 1.44.78 to 1.44.82
build(deps): bump github.com/moby/buildkit from 0.10.3 to 0.10.4
build(deps): bump helm.sh/helm/v3 from 3.9.3 to 3.9.4
ci(deps): bump goreleaser/goreleaser-action from 3.0.0 to 3.1.0
build(deps): bump github.com/mackerelio/go-osstat from 0.2.2 to 0.2.3
build(deps): bump github.com/hashicorp/hcl/v2 from 2.13.0 to 2.14.0
build(deps): bump github.com/tdewolff/minify/v2 from 2.12.0 to 2.12.1
build(deps): bump github.com/gookit/color from 1.5.1 to 1.5.2
build(deps): bump github.com/aws/aws-sdk-go from 1.44.82 to 1.44.90
build(deps): bump github.com/aws/aws-sdk-go from 1.44.90 to 1.44.91

Maintenance

docs(kicsbot): update images digest

Release

1.6.1 - 2022.09.28

- **Highlights**
- Code coverage to 80%
- Bug fixes

v1.6.1 Latest

rafaela-soares released this 8 days ago · 22 commits to master since this release · v1.6.1 · 4be6ad3

New features and improvements

added 2 queries for CloudFormation and Terraform

update(coverage): code coverage improvements (#5744)
feat(workflows): add workflow to check latest software versions (#5823)

Bug fixes

fix(query): fix query descriptionText for s3 logging disabled kms rotation and iam policies (#5810) by **@tomk-orca**
fix(query): fix queries expected value to 'should be...' (#5816) by **@liorj-orca**
fix(query): fix dockerfile security query regex (#5826)
fix(query): change s3 bucket acl grants write acp security query (#5780)
fix(query): remove string check in open api security query (#5831)
fix(query): change s3 bucket with all permissions security query (#5781)
fix(query): update s3 bucket policy accepts http requests security query (#5832)
fix(query): updated lambda_function_with_privileged_role (#5833)
fix(query): fix responses with wrong http status code security query (#5834)
fix(query): fixed Docker queries related to issues 5115, 5116, and 5118 (#5295)
fix(bug): bug in get metrics script (#5796)
fix(bug): add support for certificate body process from tfvar (#5837)
fix(terraform data source): added data resources resolver (#5839)

Dependency updates bumps

build(deps): bump github.com/GoogleCloudPlatform/terraformer from 0.8.21 to 0.8.22 (#5817) by **@tomk-orca**
build(deps): bump github.com/spf13/viper from 1.12.0 to 1.13.0 (#5766)
build(deps): bump k8s.io/client-go from 0.24.3 to 0.25.1 (#5804)
build(deps): bump github.com/aws/aws-sdk-go from 1.44.91 to 1.44.101 (#5809)
build(deps): bump github.com/open-policy-agent/opa from 0.43.0 to 0.44.0 (#5777)

ci(deps): bump actions/upload-artifact from 2 to 3 (#5764)
ci(deps): bump golang from 1.19.0-alpine to 1.19.1-alpine (#5767)
ci(deps): bump docker/setup-buildx-action from 1 to 2 (#5770)

Maintenance

chore(gitlab-ci): add --ci flag to gitlab examples (#5682) by **@sluetze**
update(docs): correct the GH action name (#5818) by **@konstruktoid**
update(docs): improve information in the configuration docs (#5829) by **@VladMasarik**

1.6.1 Release Plans

Feature Name	Due Date	Actual
BOM Support AWS RDS	Sep 2022	In review
BOM Support – AWS DynamoDB	Sep 2022	In review
BOM Support – AWS Aurora	Sep 2022	In review

Planned releases:

- **1.6.2**
  - 12 October, 2022

HacktoberFest Plans

KICS Auto-remediation add queries to new platforms:

- Ansible
- CloudFormation

Extra queries for platforms added in 1.6:

- Crossplane
- Pulumi
- Knative
- Serverless
- Alicloud

Adding support to new platforms:

- RedHat - Scanning Openshift;
- Puppet IaC tool
- AWS SecurityHub
- Microsoft Defender for Cloud

Other, TBA

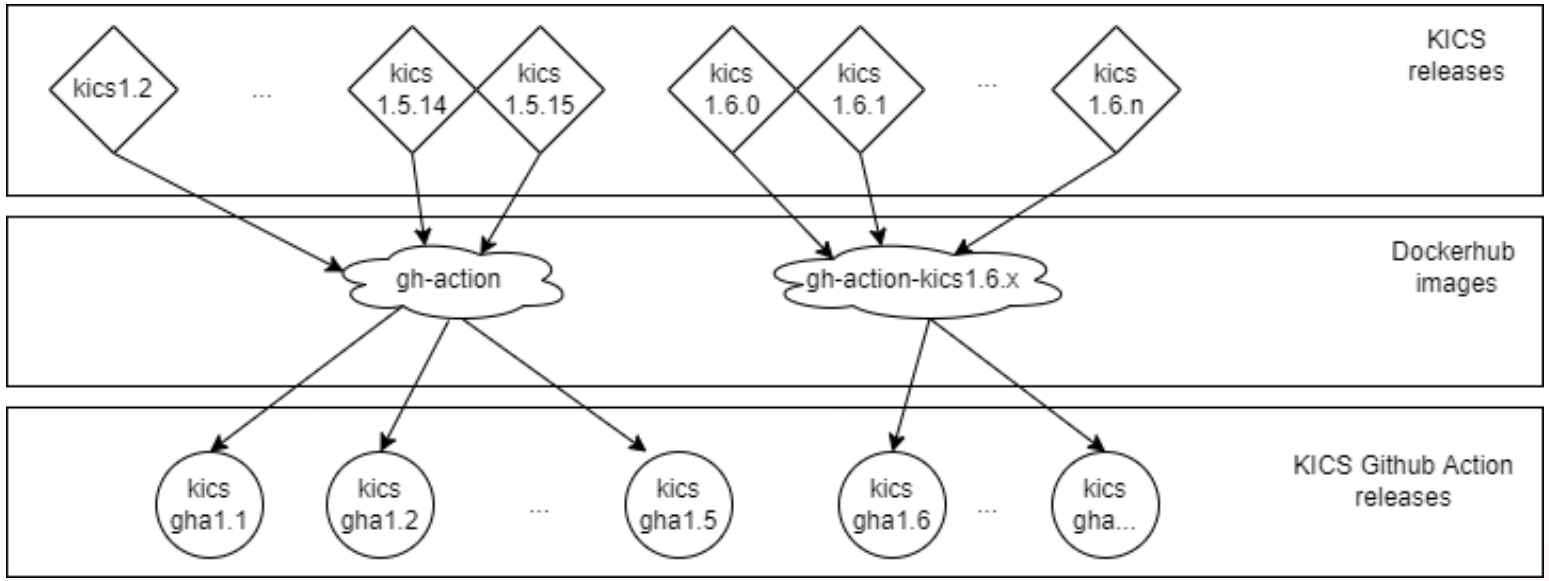
HacktoberFest Contributors

@patrickpichler with 4 contributions

@JoaoDanielRufino with 1 contribution

What is keeping us busy...

Github Action – Upgrading Process



Should KICS scan GitHub workflows?

Potential queries:

> Action not pinned to a full-length commit SHA

```
- name: KICS scan
  uses: checkmarx/kics-github-action@v1.5
  uses: checkmarx/kics-github-action@4988213cc09c75b0cfb8bb845f3734d5b662408c
```

> GITHUB_TOKEN permissions not restricted

```
1  name: "KICS"
2
3  on:
4    push:
5      branches: [ main, master ]
6    pull_request:
7      # The branches below must be a subset of the branches above
8      branches: [ main, master ]
9      paths-ignore:
10       - '**/*.md'
11       - '**/*.txt'
12   schedule:
13     - cron: '28 15 * * 3'
14
15+permissions:
16+  contents: read
```

Should KICS scan GitHub workflows?

Potential queries:

> Script injection

```
run: |
  title="${{ github.event.pull_request.title }}"
```

title"; ls $GITHUB_WORKSPACE"

> ...

Hearing from the Community

KICS.

by Checkmarx