Checkmarx

The world runs on code. We secure it.

KICS

Community Meeting

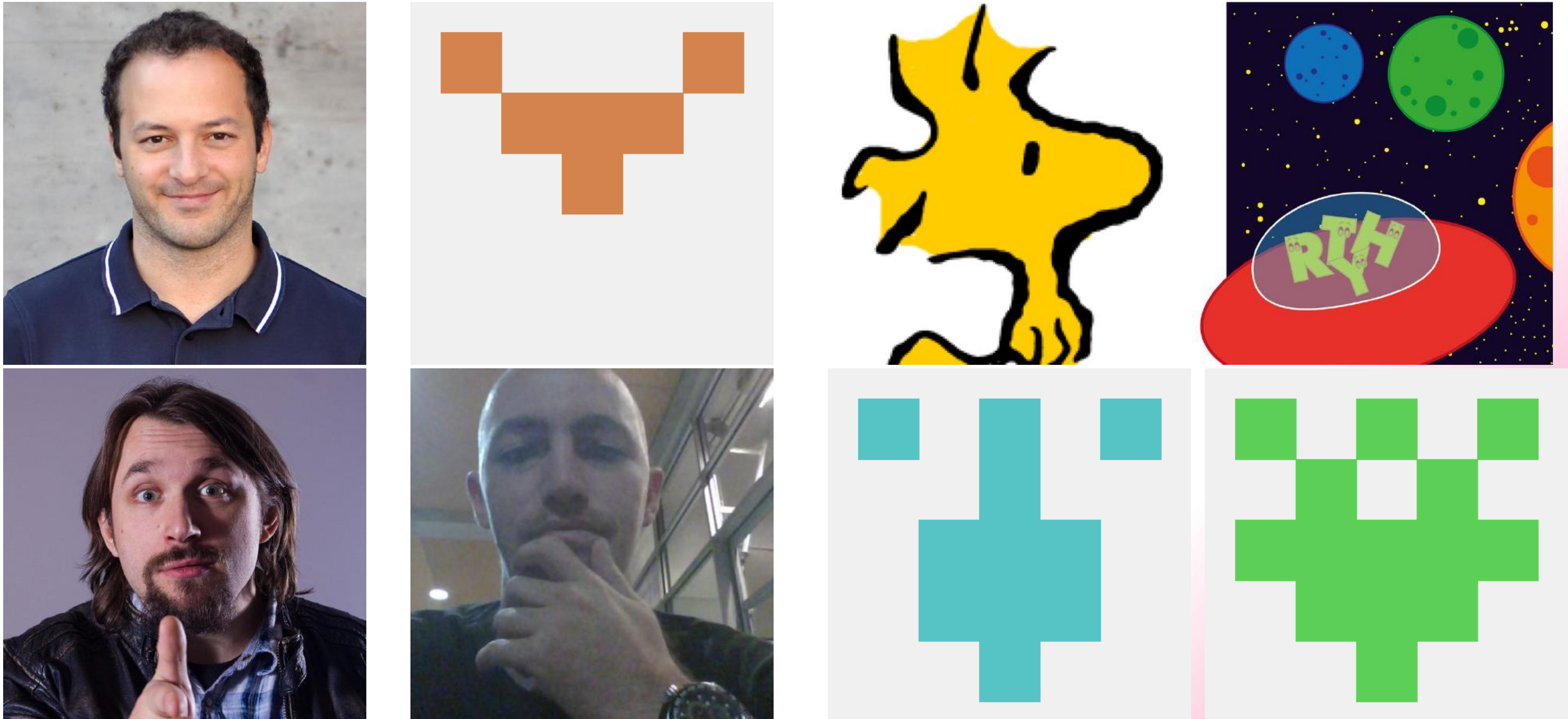
2022.09.22

kics.

by Checkmarx

Meet the KICS team

KICS contributors (2+ commits)



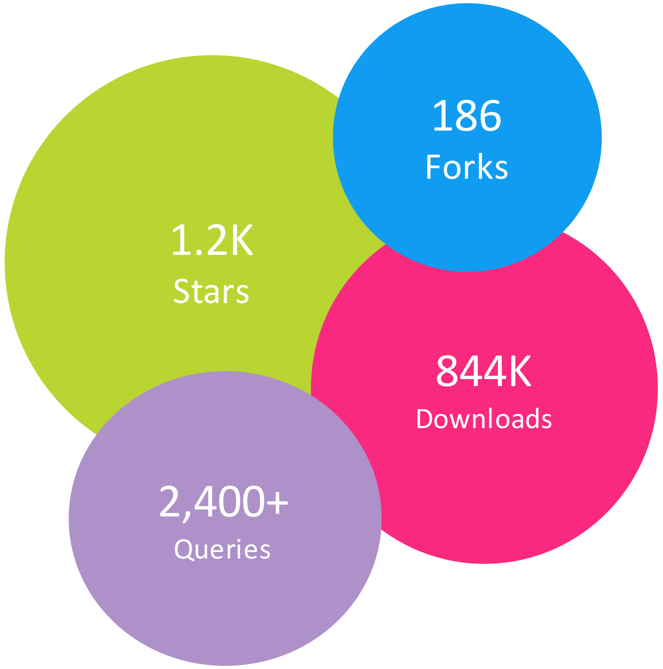
Community meetings

- **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

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 – 2022-09-22



186 Forks

1.2K Stars

844K Downloads

2,400+ Queries

KICS 1.6.0 was released

KICS GitHub Action – still in KICS 1.5.15 - Let's discuss

Community PR Merged (for KICS 1.6.1)

- add --ci flag to gitlab examples #5682 - @sluetze
- fix query descriptionText #5810 - @tomk-orca
- fix queries expected value to 'should be...' #5816 - @liorj-orca

Community PR Pending (for later version)

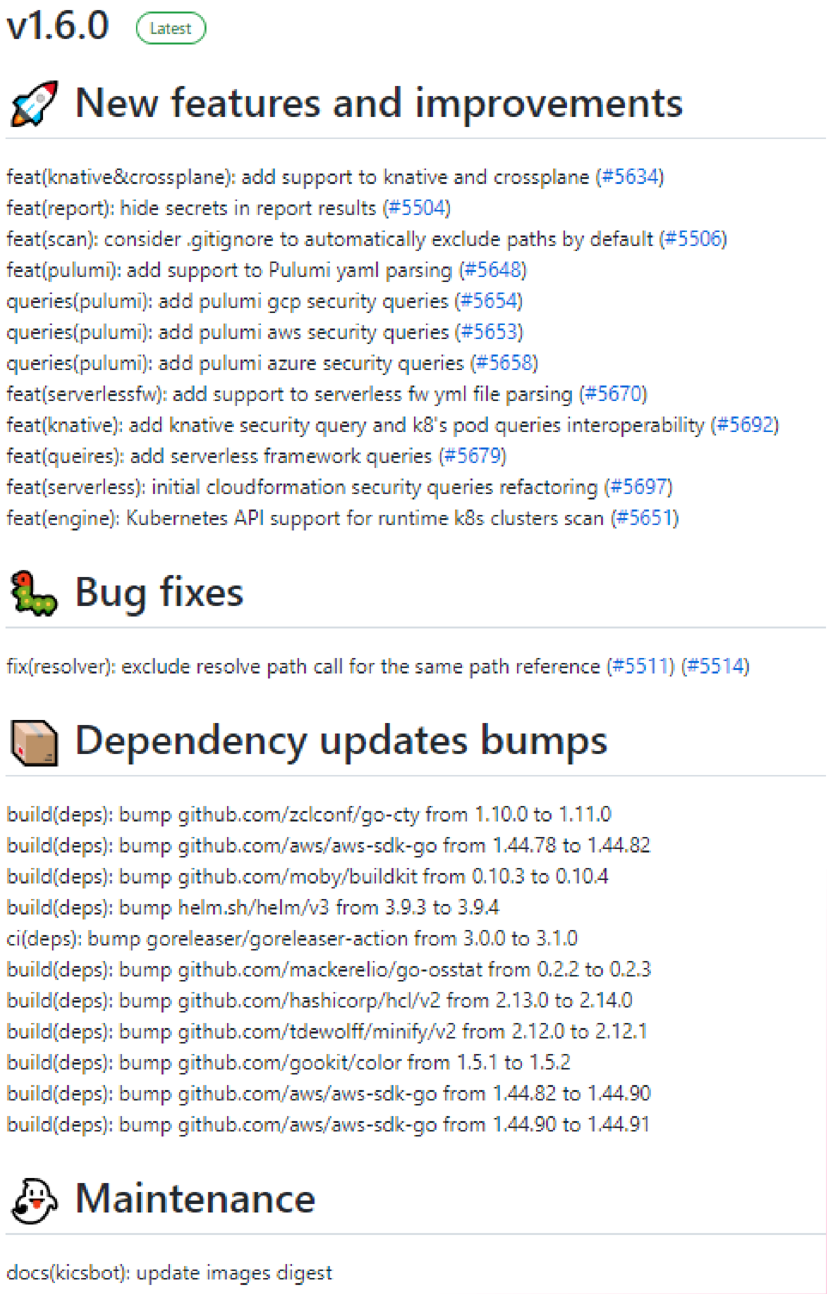
- change to use working directory when looking for `kics.config` #5319 - @lipeavelar
- bump github.com/GoogleCloudPlatform/terraformer from 0.8.21 to 0.8.22 #5817 - @tomk-orca
- correct the GH action name #5818 - @konstruktoid

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

1.6.1 Release Plans

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

Planned releases:

- **1.6.1**
  - 28 September, 2022
- 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:

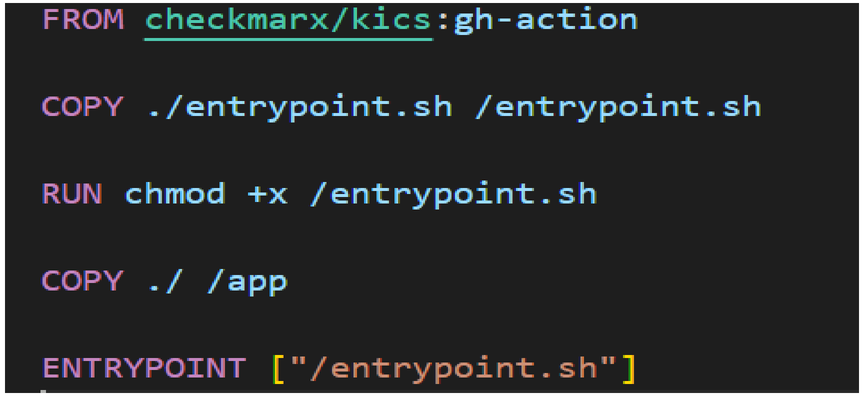
- RedHat - Scanning Openshift;
- Puppet IaC tool
- AWS SecurityHub
- Microsoft Defender for Cloud

Other, TBA

What is keeping us busy...

Github Action

The 1.5.15 vs 1.6 Dilemma

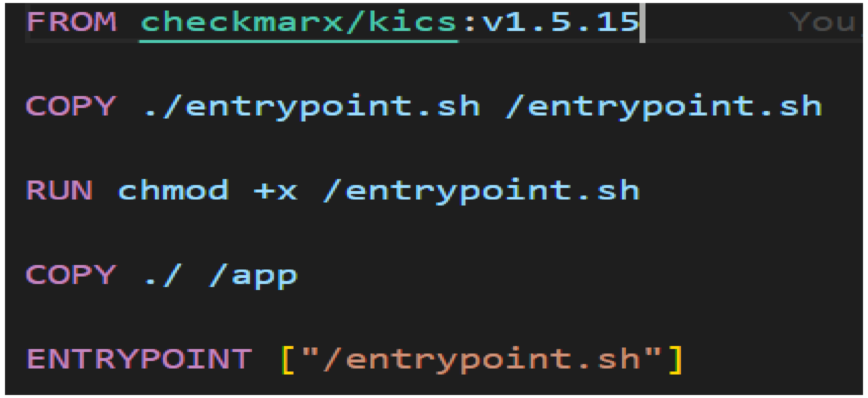


```
FROM checkmarx/kics:gh-action

COPY ./entrypoint.sh /entrypoint.sh

RUN chmod +x /entrypoint.sh

COPY ./ /app

ENTRYPOINT ["/entrypoint.sh"]
```

uses:checkmarx/kics-action@v1.3

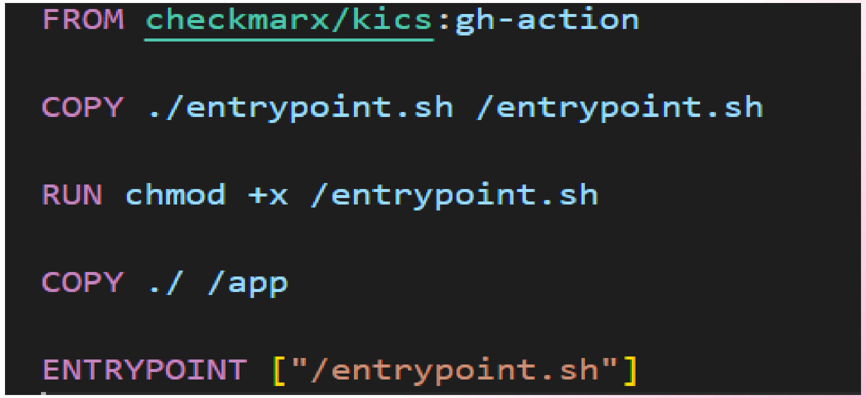
uses:checkmarx/kics-action@v1.4

uses:checkmarx/kics-action@v....



```
FROM checkmarx/kics:v1.5.15        You

COPY ./entrypoint.sh /entrypoint.sh

RUN chmod +x /entrypoint.sh

COPY ./ /app

ENTRYPOINT ["/entrypoint.sh"]
```

uses:checkmarx/kics-action@v1.5.x

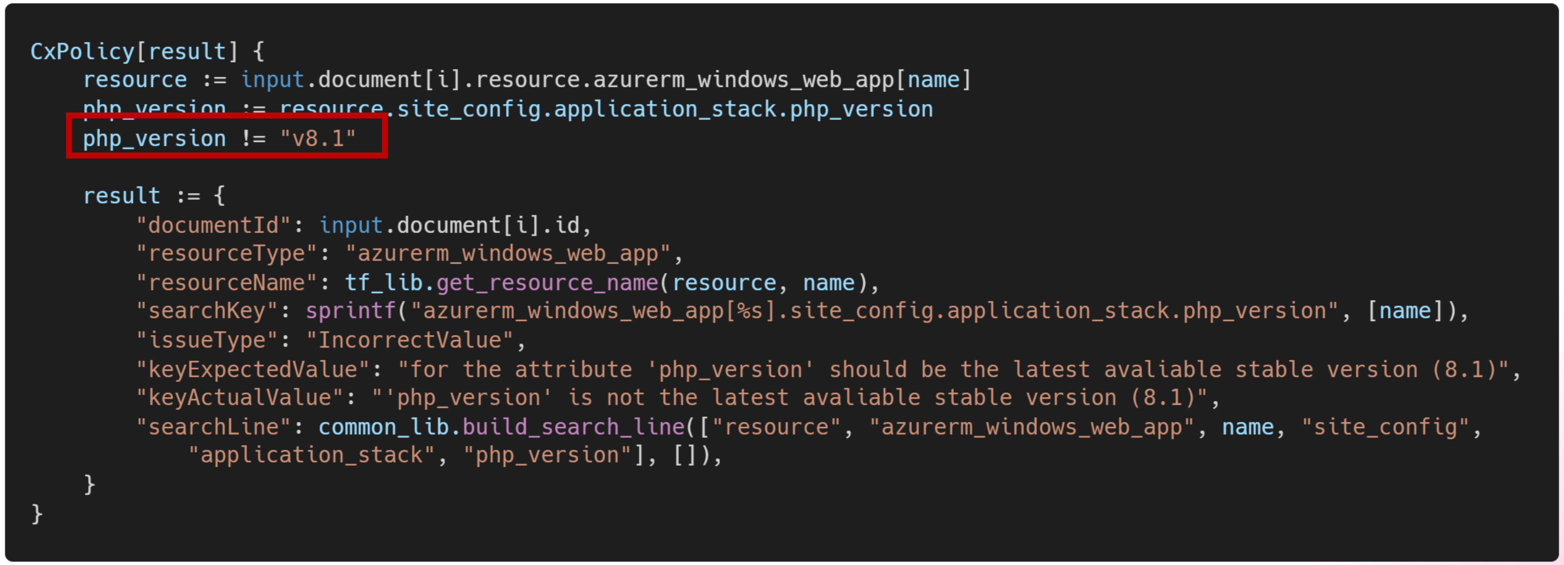


```
FROM checkmarx/kics:gh-action

COPY ./entrypoint.sh /entrypoint.sh

RUN chmod +x /entrypoint.sh

COPY ./ /app

ENTRYPOINT ["/entrypoint.sh"]
```

uses:checkmarx/kics-action@v1.6

Automatically get latest version

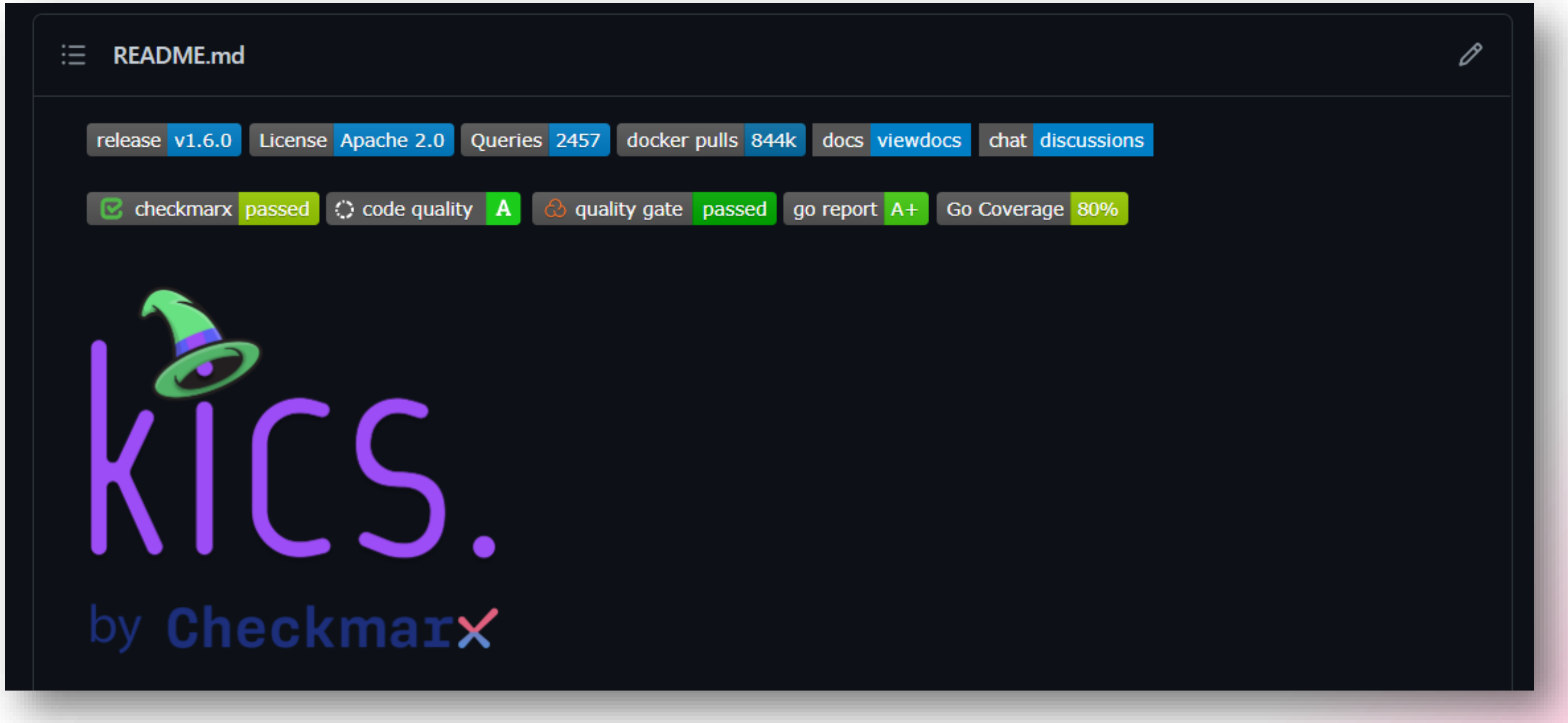
- Stop the use of magic numbers
- Add last version data in assets/libraries/common.json
- Get last version data from `endoflife.date/api`



```
CxPolicy[result] {
    resource := input.document[i].resource.azurerm_windows_web_app[name]
    php_version := resource.site_config.application_stack.php_version
    php_version != "v8.1"

    result := {
        "documentId": input.document[i].id,
        "resourceType": "azurerm_windows_web_app",
        "resourceName": tf_lib.get_resource_name(resource, name),
        "searchKey": sprintf("azurerm_windows_web_app[%s].site_config.application_stack.php_version", [name]),
        "issueType": "IncorrectValue",
        "keyExpectedValue": "for the attribute 'php_version' should be the latest avaliable stable version (8.1)",
        "keyActualValue": "'php_version' is not the latest avaliable stable version (8.1)",
        "searchLine": common_lib.build_search_line(["resource", "azurerm_windows_web_app", name, "site_config",
            "application_stack", "php_version"], []),
    }
}
```

Increase Code Coverage

- Add more unit tests
- Code Coverage back to 80%



README.md

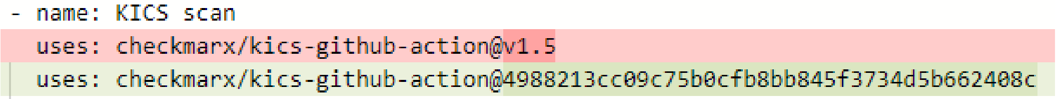
release v1.6.0 | License Apache 2.0 | Queries 2457 | docker pulls 844k | docs viewdocs | chat discussions

checkmarx passed | code quality A | quality gate passed | go report A+ | Go Coverage 80%

Should KICS scan GitHub workflows?

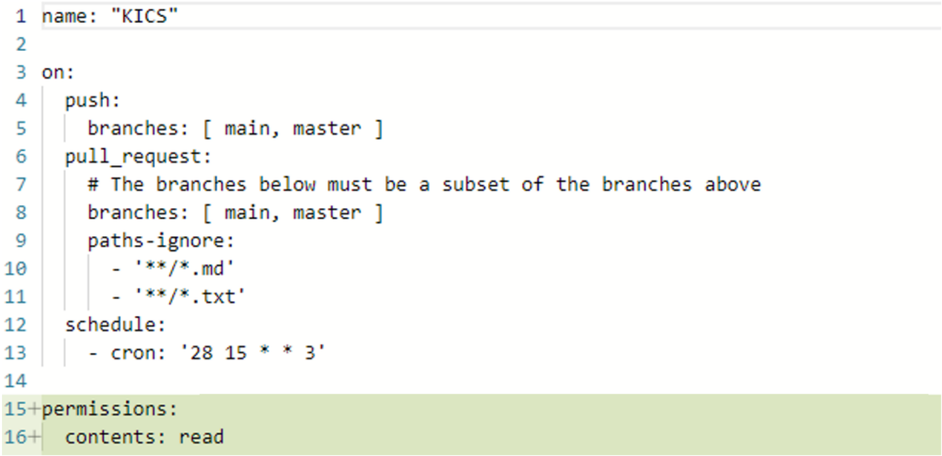
Potential queries:

- 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

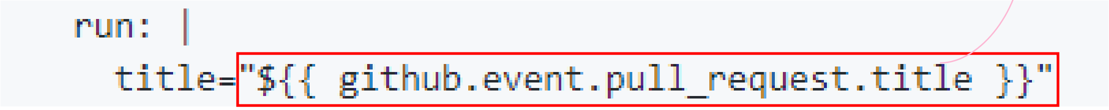


```
name: "KICS"

on:
  push:
    branches: [ main, master ]
  pull_request:
    # The branches below must be a subset of the branches above
    branches: [ main, master ]
    paths-ignore:
      - '**/*.md'
      - '**/*.txt'
  schedule:
    - cron: '28 15 * * 3'

permissions:
  contents: read
```

Should KICS scan GitHub workflows?

Potential queries:

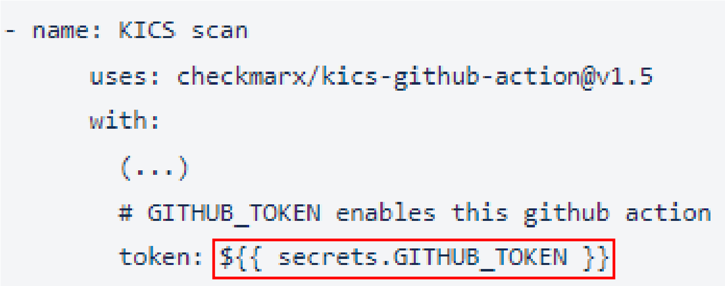
- Script injection



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

title"; ls $GITHUB_WORKSPACE"

- Secrets in use



```
- name: KICS scan
    uses: checkmarx/kics-github-action@v1.5
    with:
      (...)
      # GITHUB_TOKEN enables this github action
      token: ${{ secrets.GITHUB_TOKEN }}
```

- ...

Flags Deprecation

We are planning to deprecate some flags in KICS, during KICS 1.6.x releases.

The motivation: continuously keep "how to use KICS" documentation easy to read and follow; continuously keep KICS maintenance and improvements easy and accessible to the community.

- `--minimal-ui`
- `--no-progress`
- ~~`--preview-lines`~~ **@lior-orca** (use case: decrease it to 1 preview line, to reduce the noise)
- `--no-color`
- `--input-data`

Hearing from the Community

kics.

by Checkmarx