Checkmarx

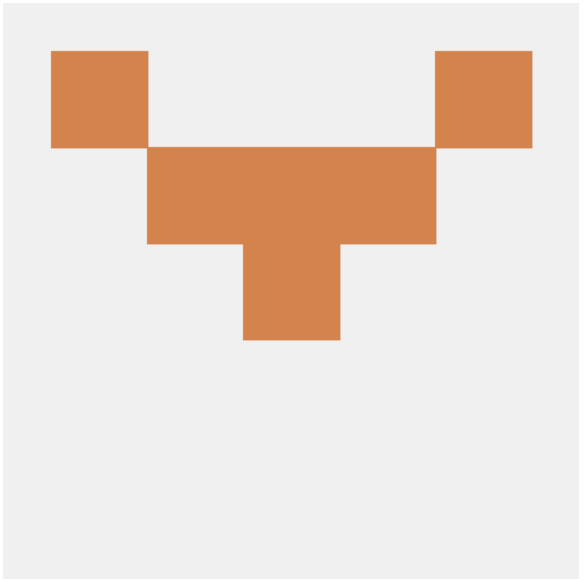
The world runs on code. We secure it.

KICS

Community Meetings

2022.08.11

KICS 1.5 contributors (2+ commits)



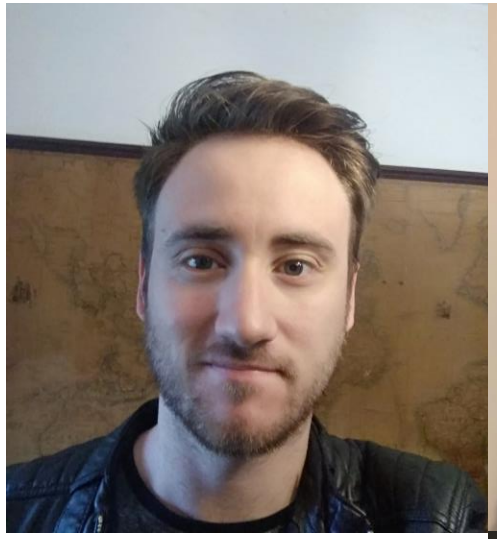
Community meetings

2022.08.11

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

Meet the KICS team





Release

1.5.13 - 2022.08.03

- **Highlights**
  - **Memory leak issue fixed**
  - **Added queries for Cloudformation**
  - **AWS BOM - resource_accessibility output updated**

v1.5.13 Latest

New features and improvements

added 4 queries for CloudFormation

Bug fixes

fix(query): azure aks rbac-variable changed (#5652) by @rndmh3ro
fix(query): azure aks policies addon var changed (#5661) by @rndmh3ro
fix(query): add missing name check in S3Bucket for AWS CloudFormation (#5642)
fix(bom): change AWS BOM resource_accessibility output values (#5639)
fix(detector): fixed memory leak (#5626)

Dependency updates bumps

build(deps): bump github.com/aws/aws-sdk-go from 1.44.55 to 1.44.59 (#5613) (#5617) (#5624) (#5628)
build(deps): bump github.com/BurntSushi/toml from 1.1.0 to 1.2.0 (#5627)
ci(deps): bump alpine from 3.16.0 to 3.16.1 (#5618)
ci(deps): bump docker/build-push-action from 3.0.0 to 3.1.0 (#5623)

Maintenance

update(docs): added KICS Auto Scanning Extension for Visual Studio documentation (#5662)

1.6 Release Plans

Feature Name	Due Date	Actual
K8S API Support – dynamic cluster scanning	Aug 2022	In Code Review
Support Pulumi (YAML only)	Aug 2022	In Code Review
Support Crossplane	Aug 2022	In Code Review
Support Serverless Framework	Aug 2022	In Progress
Support Knative	Aug 2022	In Progress
KICS Integration in Codefresh's ArgoHub	Aug 2022	In Progress

Planned releases:

- **1.5.14**
  - 17 August, 2022
- **1.6**
  - End of August, 2022 (tentative)

K8S API Support – dynamic cluster scanning

- From version 1.6, KICS calls the Kubernetes API to scan resources deployed in runtime K8s cluster. The runtime information ofthe resources is obtained by providing the K8s credentials as environment variables and a kuberneter path to KICS, via `-p` flag.

Configure K8s Credentials

> Config file

> Service Account Token

> Certificate

Define kuberneter path

kuberneter::{namespaces}:{apiVersions}:{kinds}

Example

```
docker run
-v <credentials_path>:/credentials -v ${PWD}:/path/
-e K8S_CONFIG_FILE=/credentials/<config-file-name>
checkmarx/kics:v1.5.6 scan -p "kuberneter::*:*:*"  -v --no-progress -o /path/results
```

K8S API Support – dynamic cluster scanning

Technology Support

- Pulumi (Yaml)
  - What is it
    - IaC code platform that uses popular programming languages
    - Pulumi YAML
  - Support
    - 16 Security Queries
    - 3 Cloud Providers
    - Kubernetes

- Crossplane
  - What is it
    - Kubernetes add-on
    - Assemble infrastructure from multiple vendors
  - Support
    - 15 Security Queries
    - 3 Cloud Providers

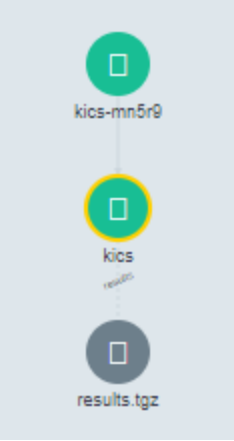
- Serverless Framework
  - What is it
    - Deploy and manage serverless applications
    - AWS default provider
  - Support
    - 10 Security Queries based on existing AWS SAM Security Queries
    - Refactor AWS CloudFormation Security Queries to allow interoperability

- Knative
  - What is it
    - Serverless Containers in Kubernetes environment
  - Support
    - 1 Security Query for Knative Eventing
    - Add interoperability with existing k8s Pod Security Queries

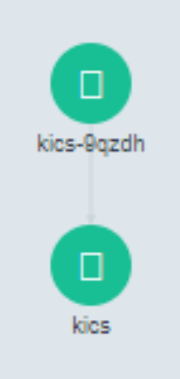
KICS Integration in Codefresh's ArgoHub

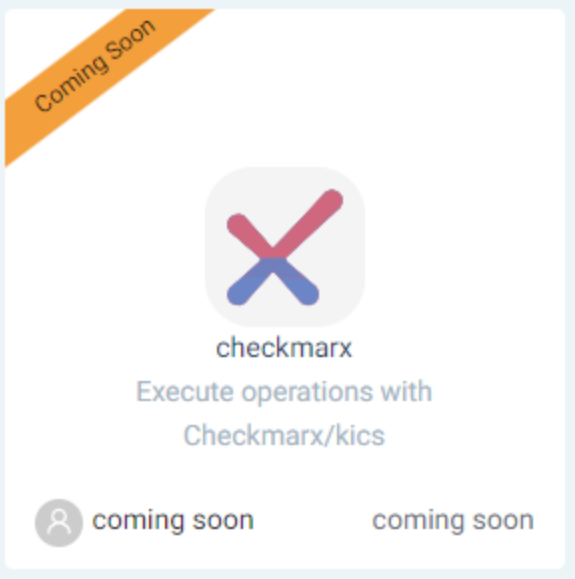
It will be available two KICS workflowTemplates:

- **kics-scan-report**: runs KICS against a IaC project/file and generates a KICS report



- **kics-scan**: runs KICS against a IaC project/file





https://codefresh.io/argohub/

KICS Integration – Visual Studio plugin

- **Overview**
  - Checkmarx's KICS Auto Scanning extension for VS Code initiates KICS scans directly from their VS Code console. The scan runs automatically whenever an infrastructure file of a supported type is saved, either manually or by auto-save. The scan runs only on the file that is open in the editor.

- **Main Features**
  - Free tool, no Checkmarx account required
  - Run scans directly from your IDE
  - Scans are triggered automatically whenever a file is saved

- **Prerequisites**
  - You must have Docker installed and running in your environment

Hearing from the Community

- Johannes Feichtner (Churro) about RBAC & other contibutions
- Gafnit (gafnit-lightspin) about AWS IAM privilege escalation
- Open floor for other participants

KICS.

by Checkmarx