Checkmarx

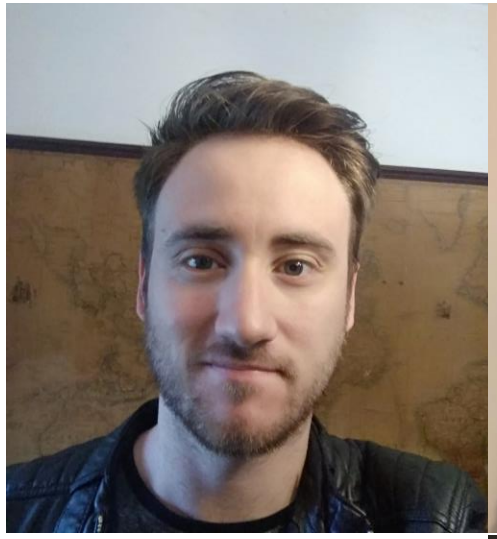
The world runs on code. We secure it.

KICS

Community Meeting

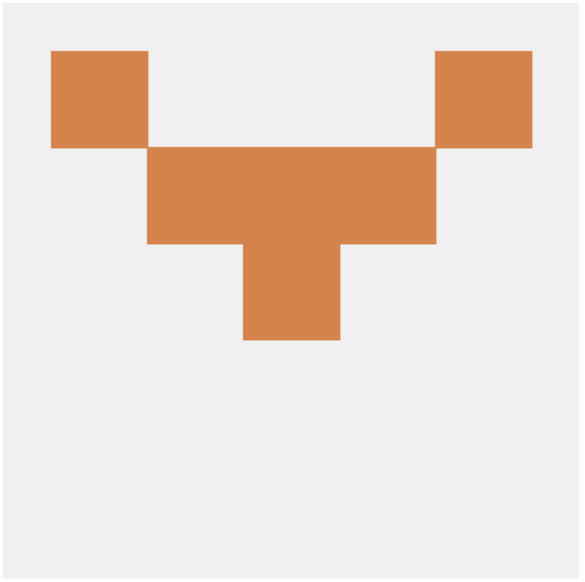
2022.08.25

Meet the KICS team





KICS 1.5 contributors (2+ commits)



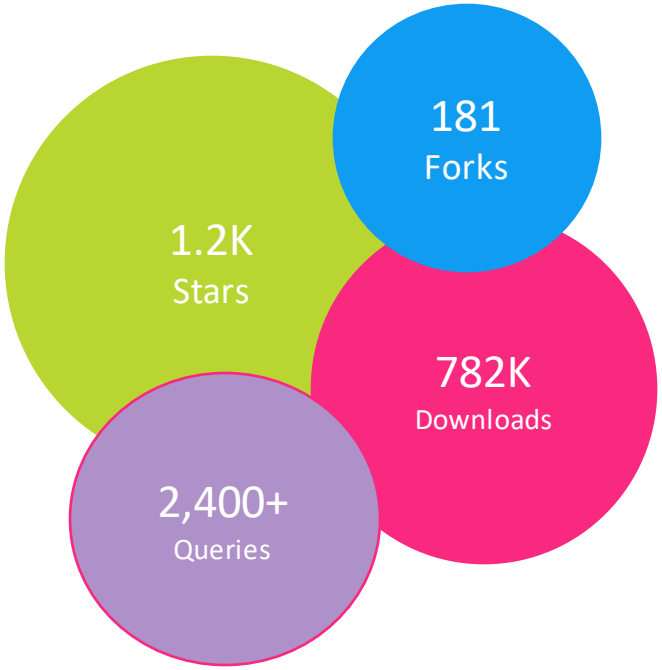
Community meetings

2022.08.25

- **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 1.5 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



KICS 1.5.14 was released

KICS Github Action – updated to KICS 1.5.14

Community PR Merged (for KICS 1.5.15)

+ cloudformation-aws queries convert to a recommendation rather than a current status #5647 - @liorj-orca
+ cloudformation-aws queries convert to a recomm... #5646 - @liorj-orca
+ align queries cross different platforms #5539 - @roi-orca
+ add new aws iam privilege escalation queries #5423 - @gafnit-lightspin

Community PR Pending (for later)

+ change to use working directory when looking for `kics.config` #5319 - @lipeavelar
+ add --ci flag to gitlab examples #5682 - @sluetze

Release

1.5.14 - 2022.08.17

- **Highlights**
  - Added resolver for Docker Args
  - Added parentheses expression to convertStringPart in Terraform
  - Improved the complexity of Terraform query '*lambda_function_with_previleged_role*'
  - Several queries' issues fixed

v1.5.14 Latest

Bug fixes

fix(query): change approach in api_gateway_with_cloudwatch_logging_disabled security query for terraform aws (#5693)
fix(queries): change queries metadata to remove the inconsistency (#5702)
fix(query): improve RegEx rule in curl_or_wget_instead_of_add (#5706)
fix(query): update_instruction_alone (#5707)
fix(docker parser): added resolver for args (#5696)
fix(tf parser): added parentheses expr to convertStringPart (#5695)
fix(query): reduced complexity of 'lambda_function_with_privileged_role' query (#5686)

Dependency updates bumps

build(deps): bump golang.org/x/tools from 0.1.11 to 0.1.12 (#5640)
build(deps): bump github.com/aws/aws-sdk-go from 1.44.59 to 1.44.70 (#5672)
build(deps): bump github.com/open-policy-agent/opa from 0.42.2 to 0.43.0 (#5655)
build(deps): bump helm.sh/helm/v3 from 3.9.1 to 3.9.2 (#5632)

Maintenance

update(docs): update integrations_auto_scanning_visual_studio.md (#5673)

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	Merged
Support Crossplane	Aug 2022	Merged
Support Serverless Framework	Aug 2022	In Code Review
Support Knative	Aug 2022	Merged
KICS Integration in Codefresh's ArgoHub	Aug 2022	Under Approval

https://github.com/Checkmarx/kics/tree/release/1.6

Planned releases:

- **1.5.15**
  - 31 August, 2022
- **1.6**
  - 14 September, 2022

WIP - Community Issues - Highlights

Issue: Ansible include causes kics to ignore it's ignore patterns (#5685) - @sluetze

Problem: KICS is not considering any comment in YAML files, when it finds a file to resolve. This happens because KICS unmarshal the content and marshal the resolved content in any variable, which loses the "comments information".

Solution: We will specify the variable as yaml.Node to keep the comments.

Limitation: Password and Secrets only analyzes the original content. So, it should only consider the lines to ignore related to the original content and not to the resolved content. [We are working on that]

WIP - Community Issues - Highlights

Issue: Error getting policy present in data type source for Terraform parser leading to FP's (#5489) - @dalenewman

Problem: Inside the KICS Terraform parser when policies are targeted and specified in a data type block a decode is made to incorporate the referenced policy in the original resource. Due to Terraform resource referencing being deemed as variables in hcl decode function some diagnostic errors are returned specifying that variable is missing in evaluation context passed as argument. Once the detections of diagnostic errors is made the policy is returned as empty string.

Solution: Check for the diagnostic errors type, if it is only "Unknown variable" the policy is returned with the original string value in the variable in question.

WIP - Community Issues - Highlights

Query issues that we are working on:

- "IAM Database Auth Enabled must be configured to true" Flagging for Oracle DBs but Cannot be Configured (#5711) - @adamkendall1
- False positive: terraform ec2_instance_has_public_ip (#5643) - @jpriebe
- TF IaC - AWS IAM Policy Check not Compatible with Resources that Don't support ARNs (#5714) - @adamkendall1

KICS VSCode Extension

Auto scan & Auto remediation

Live Demo

Hearing from the Community

- **Open floor for all participants**

KICS.

by Checkmarx

THANK YOU!