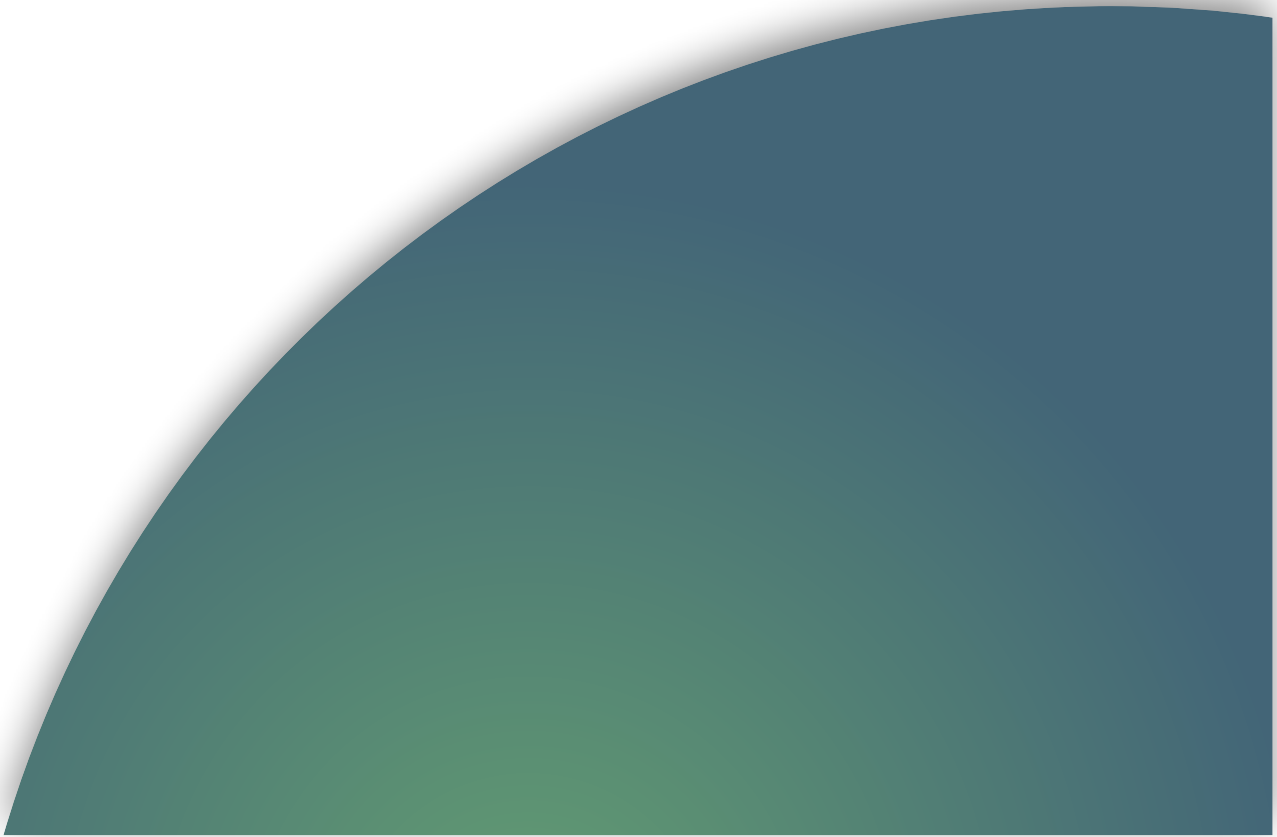


Usually C.I. / C.D. system stores sensitive information.

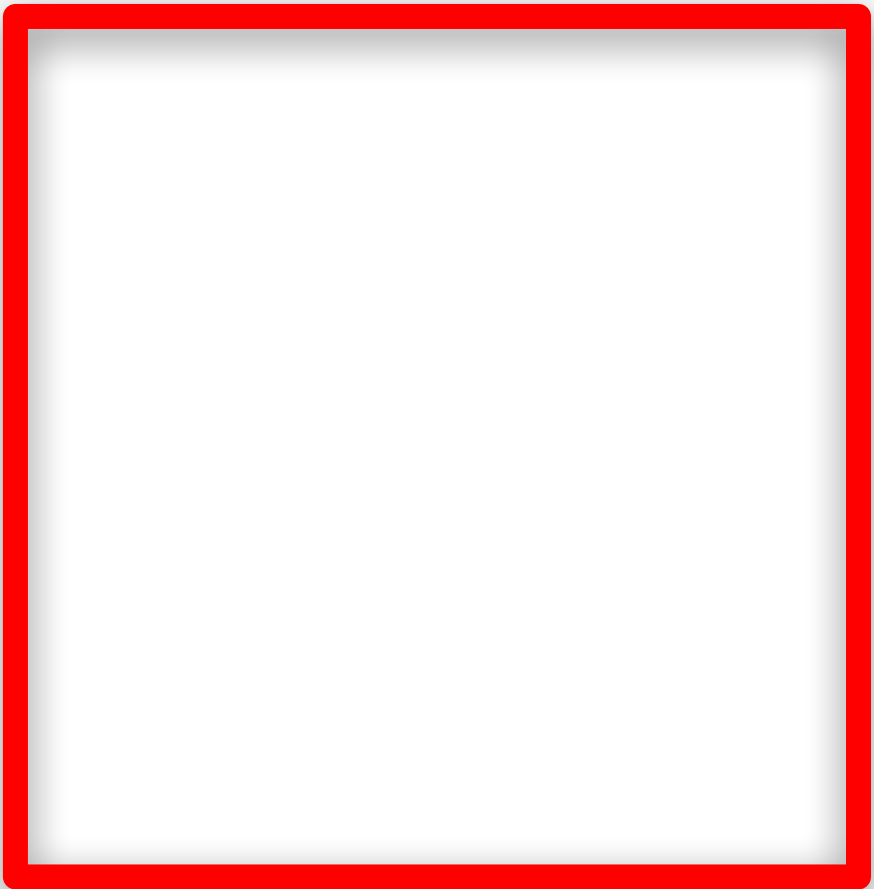
They need them to access to productive environments, publish artefacts, perform some checks, etc

They, usually, store as environment vars.

https://docs.gitlab.com/ee/ci/variables/

Don’t trust third party GitHub Actions

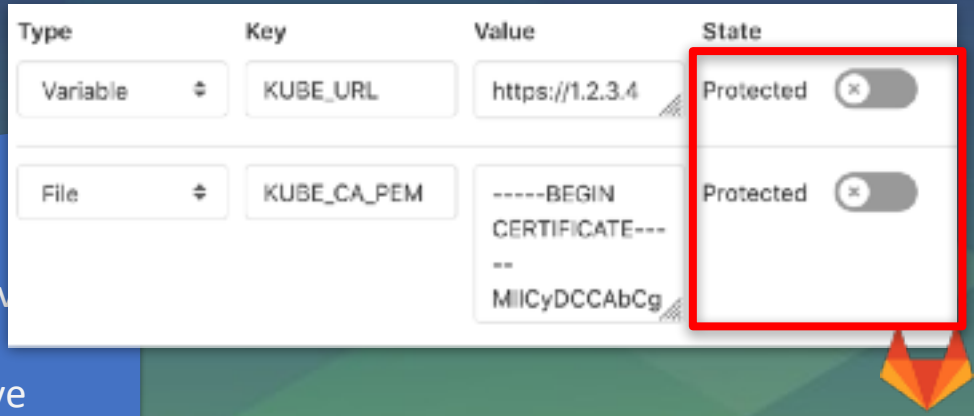

Type
Key
Value
State
Variable
KUBE_URL
https://1.2.3.4
Protected
File
KUBE_CA_PEM
-----BEGIN CERTIFICATE-----
MIICyDCCAbCg
Protected



The Evil GitHub Actions!

CodeCov:
https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/

The Evil GitHub Actions!



- Usually C.I. / C.D. system stores sensitiv information.
- They need them to access to productive environments, publish artefacts, perform some checks, etc
- They, usually, store as environment vars.

Don't trust third party GitHub Actions

CodeCov: https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/

https://docs.gitlab.com/ee/ci/variables/

A reverse Shell in the Pipeline

- What if an user can execute anything in a Pipeline?
- What if the C.I. has not limited the output traffic?

https://alionder.net/jenkins-script-console-code-exec-reverse-shell-java-deserialization/