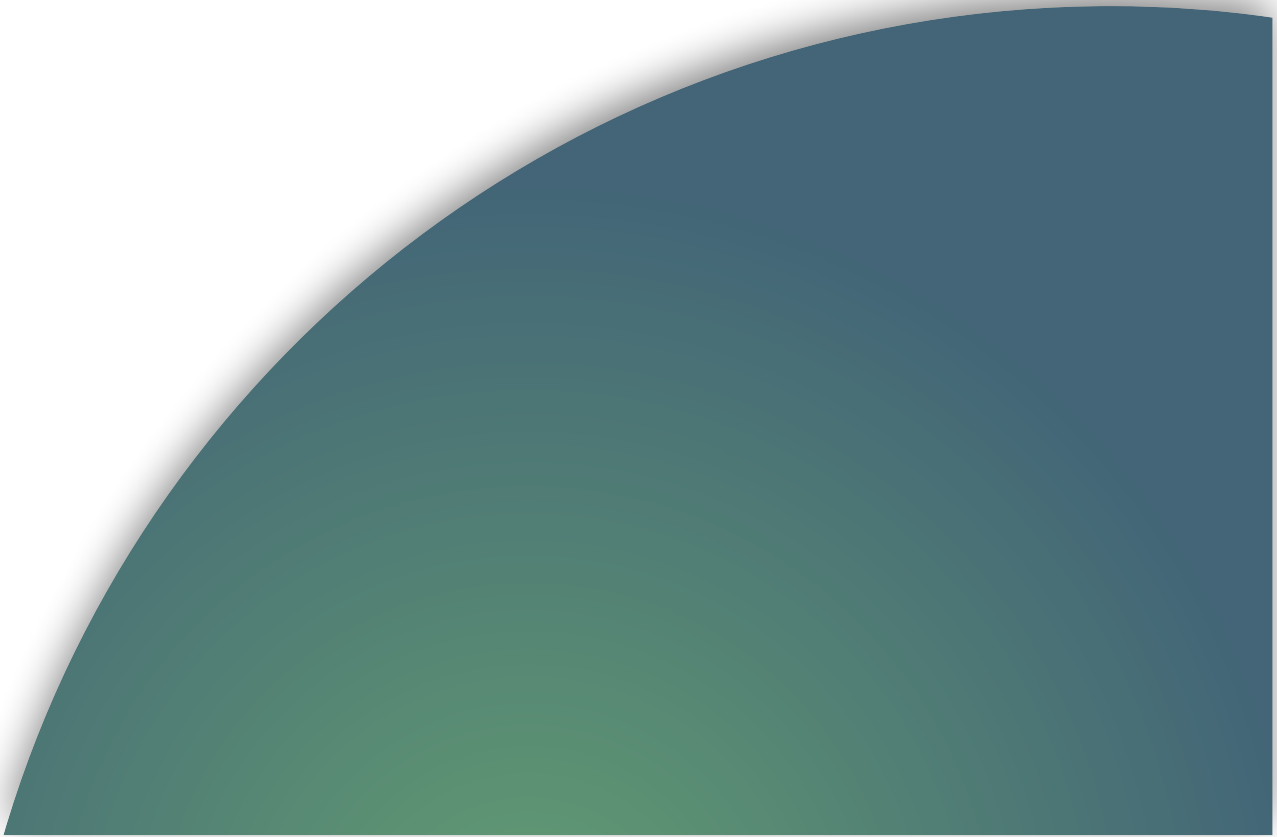

What if a developer can publish an arbitrary code into artefacts / libraries repository?

What if a developer publish a trojanized version of a library?

What if a developer publish, intentionally, an artefact with known vulnerabilities?

You must control who and what publish in the artefact repository


STOP

Control Artefacts Repository

Control Artefacts Repository

- What if a developer can publish an arbitrary code into artefacts / libraries repository?
- What if a developer publish a trojanized version of a library?
- What if a developer publish, intentionally, an artefact with known vulnerabilities?

You must control who and what publish in the artefact repository

The ENVIRONMENT Leak! (1/2)

- 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.