ARMO

The Makers of Kubescape

Compliance case study

Gitpod

Achieving SOC 2 compliance with ARMO

Compliance without sacrificing security

Gitpod

Gitpod is an open-source Kubernetes application for ready-to-code cloud development environments. It spins up fresh, automated development environments for each task, in the cloud, in seconds. It enables users to describe the development environment as code and start instant and remote cloud development environments directly from a browser or desktop IDE.

Company size
11-50 employees

Industry
Information Technology & Services

Challenge

Gitpod serves customers of many sizes from all over the world. These days, many customers are security concerned and are looking to providers for independent assurance about appropriate security safeguards. To this end, Gitpod went through the process of achieving SOC 2 compliance. As it is considered the gold standard of security and is recognized by companies in the US and in Europe.

Problem

Part of achieving SOC 2 compliance requires setting up a vulnerability management program for infrastructure. This includes vulnerability scanning. Organizations are free to select the solutions that work best for them. The problem with finding the right solution was that many available solutions are not Kubernetes-native. As such, their findings, though valuable for the audit, are not Kubernetes-native and still leave security gaps.

Solution

Gitpod selected ARMO Platform, which is based on Kubescape - the leading open-source Kubernetes security tool - in order to get deep, Kubernetes-relevant findings, with a high signal to noise ratio. It was a perfect solution to assess potential weaknesses.

The SOC 2 auditor accepted ARMO Platform and its implementation in the SOC 2 process. The scanning reports generated by ARMO Platform were presented to the SOC 2 auditor, as part of the audit process.

To get relevant findings the team at Gitpod preferred a solution that can give insight from outside the cluster, but also from within.

ARMO Platform has become part of the security processes at Gitpod and is used at least once a week.

3 recognized frameworks

SOC 2 compliance based on: NSA-CISA; CIS Benchmark; MITRE ATT&CK

>217 security controls

Test for misconfigurations and vulnerabilities

Daily scans

Protect us from configuration drift

Quarterly review

Pinpoint areas for security improvement

> "**We chose to adopt ARMO Platform,** as it is dedicated to Kubernetes security and therefore provides us with a high signal to noise ratio."

Mirco Kater
Information Security Officer

Book a demo

Get a free risk audit

armosec.io

github.com/kubescape