ARMO

The Makers of Kubescape

Security upskilling case study

Energi Danmark

Day 0 Kuberentes security

Unlocking Kubernetes security mastery

Energi Danmark®

Energi Danmark Business Support (EDBS) is a subsidiary of Energi Danmark, providing various business services, including IT, to the multi-national energy group. They recently adopted Kubernetes to future-proof their applications, aiming for flexible and scalable application deployment.

Company size
201-500 employees

Industry
Energy and gas

Challenge

Adopting Kubernetes at scale, towards production is a complex project. It includes:

Planning the Kubernetes deployment, including selecting the right infrastructure and defining the requirements for the cluster.

Installing and configuring the Kubernetes software, including setting up the control plane and worker nodes.

Configuring the network and storage for the Kubernetes cluster, including defining how applications will be exposed and how data will be stored and accessed.

Defining policies and security settings, such as access control policies, network policies, and encryption settings.

This requires upskilling infrastructure and operations personnel on these different aspects and creating processes for the users of the infrastructure.

Problem

Kubernetes is a new infrastructure that requires a new understanding of infrastructure and operations. While a lot of the installation and configuration was allocated to a third party, security was left to be dealt with in-house. The team at EDBS knew that if they left security to a late phase in the project, it may put timelines at risk. As a result, they decided to implement security at day zero.

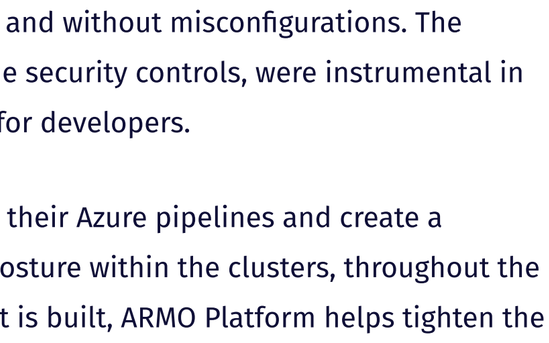
Solution

EDBS selected ARMO Platform, in order to learn how to strengthen the security posture of a Kubernetes cluster. The DevOps team initially scanned deployment files in order to mine best practices for writing them correctly and without misconfigurations. The remediation advice and the descriptions of the security controls, were instrumental in achieving comprehensive security guidelines for developers.

The next step was to plug ARMO Platform into their Azure pipelines and create a feedback loop of strengthening the security posture within the clusters, throughout the DevOps pipeline. Everytime a new deployment is built, ARMO Platform helps tighten the Kubernetes security posture by highlighting misconfigurations.

The final step (to-date) was to run in-cluster scanning to ensure there are no vulnerabilities in the cluster.

In the future, as part of the security guidelines and to reduce developer friction, the team will endeavor to introduce ARMO platform security plug-ins (e.g. VSCode, kubectl, GitHub actions, etc.) to developers in order to reduce the reliance on written guidelines and embed them in the developer stack. Thus, reducing friction and keeping software delivery fast and agile.



>217 security controls

Test for misconfigurations and vulnerabilities

30 minutes

From set-up in CI/CD pipeline to test results

> “ARMO helps us to strengthen the security of deployments and the cluster overall. It is very easy to use and it gives a great overview of security vulnerabilities and helps us mitigate them.”

Morten Hansen
DevOps

Get a free risk audit

Book a demo

armosec.io

github.com/kubescape