Exercise 4.2: Create a Co-sign Policy to allow Signed Dockerhub Images

Now that we’ve talked about how to write policies, use them with compliance at the point of change, and the importance of supply chain security, apply what you’ve learned and write a zero trust policy that enforces our requirements and can be reused as a Compliance controller. To do this, you’ll need to use a tool called Cosign. Cosign is a project managed by Sigstore, a governing body within the OpenSSF (Open Source Security Foundation).

Also, consider how you might write a policy that enforces our image security concerns, from code signing to image signing.

Note: You can learn about Software Supply Chain security in great detail by learning more about the projects within Sigstore and the OpenSSF.

Solution