Bachelor Thesis: Securing the Software Development Life Cycle

Company: Norges Bank Investment Management (NBIM)

Address: Bankplassen 2
P.O. Box 1179 Sentrum
NO-0107 Oslo, Norway

Contact person: Astri Marie Ravnaas, +47 91 69 07 85, astri.marie.ravnaas@nbim.no

Background

Securing the Software Development Lifecycle (SDLC) is about ensuring security at the different stages of software development. This includes from planning through implementation and running in production. In order to accommodate frequent deployments to production, it is important to automate the security testing by building it into the deployment pipeline. The security testing can further benefit from shift-left, where testing is done as early as possible in the pipeline. The user experience is another important aspect. How to best secure the SDLC is a large and actively developed area with a lot of interest from the industry. Systemizing the state of the art and demonstrating how certain tools and techniques fit together will have value both to NBIM and other organizations.

Goal

Create a report outlining how to best secure parts of the SDLC. We want to focus on the deployment pipeline, from submitting new code to GitHub to deploying it to AWS. It should be based on reviewing different tools, as well as implementing a proof of concept demonstrating how the different tools can be used together. The proof of concept should demonstrate how we can maintain integrity of the code throughout the pipeline, as well as scanning for security misconfiguration and vulnerabilities at key stages of the pipeline. The user experience and ability to scale to an enterprise environment should be taken into consideration.

Summary

- Use GitHub to host source code and AWS as deployment environment.
- Evaluate relevant security tools and create a proof of concept demonstrating how the tools can be integrated together.