<Data visionaries>

- Pujun Xie
- Terlo Adam
- Syed Ali

Project statement

To enhance the security of DevOps and MLOps, we are going to develop a container scanning service which can integrate into the CI/CD pipeline of DevOps and MLOps. Container scanning refers to analyzing the contents and build process of container images to detect security issues such as vulnerabilities and faulty practices. It can be as a first line of defense which helps us detect security issues and stop them before they are exploited. In addition, it is easy to implement and can be CI/CD automated. So, it is one of the most essential workflows for secure DevOps and MLOps.

Project repo: <https://github.com/xpjllk38324/Container-Security-Scanning-Service>

This report: <https://github.com/xpjllk38324/Container-Security-Scanning-Service/blob/main/Product%20Definition/Product%20Definition.pptx>

Roles

DevOps Engineer

DevOps engineers can integrate our service into the products for improving safety.

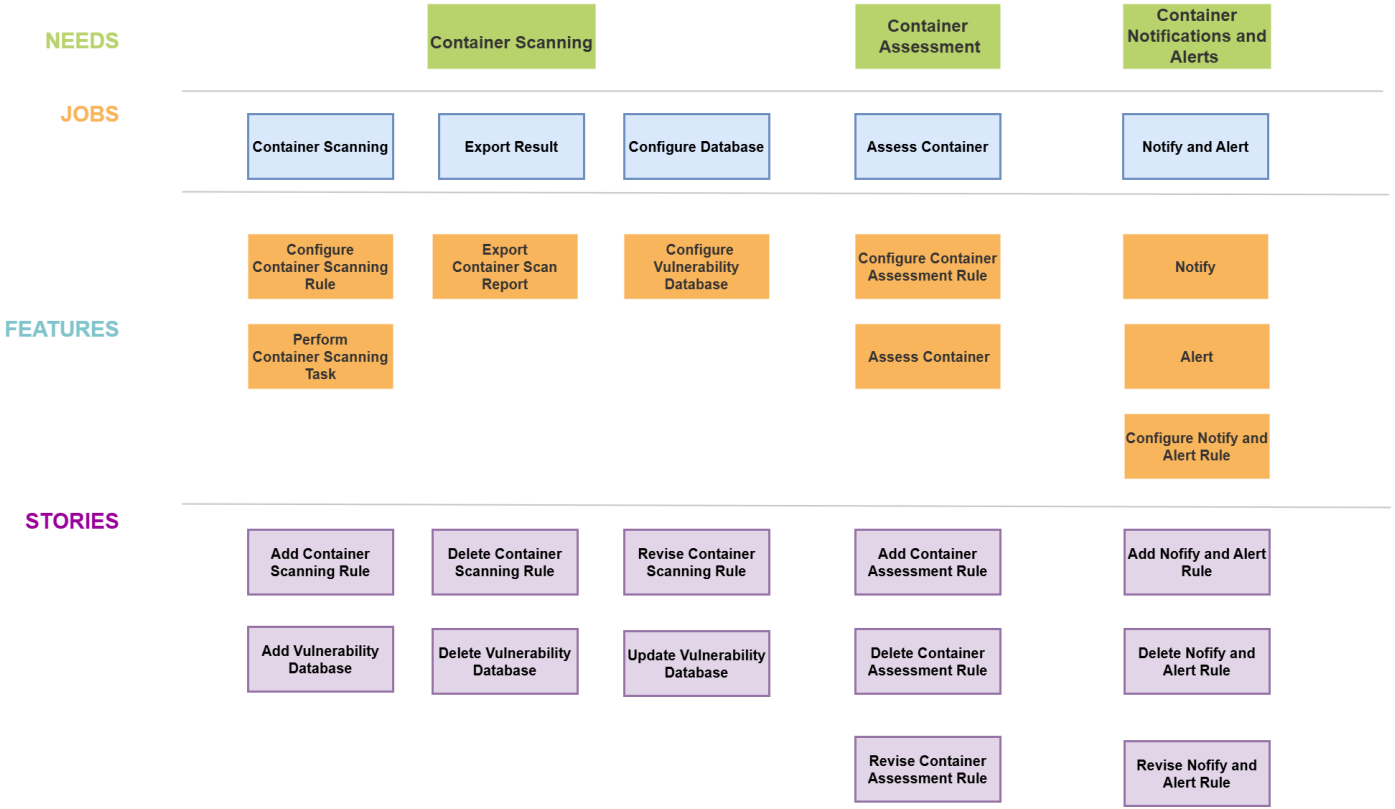
Developer

Developers can use our service to improve the safety of application.

Information Security Engineer

Information security engineers can use our service to conduct container security test.

Storymap


NEEDS
Container Scanning
Container Assessment
Container Notifications and Alerts
JOBS
Container Scanning
Export Result
Configure Database
Assess Container
Notify and Alert
FEATURES
Configure Container Scanning Rule
Export Container Scan Report
Configure Vulnerability Database
Configure Container Assessment Rule
Notify
Perform Container Scanning Task
Assess Container
Alert
Configure Notify and Alert Rule
STORIES
Add Container Scanning Rule
Delete Container Scanning Rule
Revise Container Scanning Rule
Add Container Assessment Rule
Add Nofify and Alert Rule
Add Vulnerability Database
Delete Vulnerability Database
Update Vulnerability Database
Delete Container Assessment Rule
Delete Nofify and Alert Rule
Revise Container Assessment Rule
Revise Nofify and Alert Rule