

Product name:

Data visionaries

List of team members:

Pujun Xie, Terlo Adam, Syed Ali

Product description:

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.

Feature list:

1. Configure container scanning rules. Users can configure personalized settings for the container vulnerability scanning tools.
2. Perform container scanning tasks. Users can perform container scanning task according to the configured rules.
3. Assess container security. According to the result of the container's scanning, the container vulnerability scanning service will assess container security.
4. Configure container security assessment rules. Users can set custom policy for the container security assessment.
5. Export container scan reports. Users can generate and get detailed reports containing scan results, vulnerability details and more.
6. Notify and alert. Users can get notifications and alerts in real time via email, SMS, and other channels.
7. Configure notify and alert rules. Users can set custom notify and alert rules, such as immediate notification when a high-risk vulnerability is detected.
8. Update of vulnerability database. Users can update the vulnerability database which container scanning tools use.

Constraints:

1. Container scan engine needs to quickly and accurately identify security vulnerabilities and bad practices in containers.
2. Container scanning service needs to be integrated with existing CI/CD systems, which requires services with flexible architectures capable of supporting multiple integration approaches.
3. Container scanning service needs to ensure the security and privacy of user data. The service needs to take appropriate encryption measures to protect sensitive information during data transmission and storage.