

User Cases:

1. configure container scanning rule:

1.1 Use case name: add container scanning rule

Use case number: 001

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor adding a new container scanning rule.

Triggers: The use case is triggered when the new container scanning rule is added.

1.2 Use case name: delete container scanning rule

Use case number: 002

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor deleting a container scanning rule.

Triggers: The use case is triggered when a container scanning rule is deleted.

1.3 Use case name: revise container scanning rule

Use case number: 003

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor revising a container scanning rule.

Triggers: The use case is triggered when a container scanning rule is revising.

2. perform container scanning tasks:

2.1 Use case name: perform container scanning task

Use case number: 004

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor performing container scanning task.

Triggers: The use case is triggered when a container scanning task is performed.

3. assess container:

3.1 Use case name: assess container

Use case number: 005

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor assessing a container.

Triggers: The use case is triggered when a container is assessed.

4. configure container assessment rules:

4.1 Use case name: add container assessment rule

Use case number: 006

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor adding a new container assessment rule.

Triggers: The use case is triggered when a new container assessment rule is added.

4.2 Use case name: delete container assessment rule

Use case number: 007

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor deleting a container assessment rule.

Triggers: The use case is triggered when a container assessment rule is deleted.

4.3 Use case name: revise container assessment rule

Use case number: 008

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor revising a new container assessment rule.

Triggers: The use case is triggered when a container assessment rule is revised.

5. export container scan reports:

5.1 Use case name: export container scan report

Use case number: 009

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor exporting the container scan report.

Triggers: The use case is triggered when the container scan report is exported.

6. notify and alert:

6.1 Use case name: notify

Use case number: 010

Actor: DevOps Engineer

Use case description: This use case describes the behavior of an actor getting the notification.

Triggers: The use case is triggered when the container scan report is exported.

6.2 Use case name: alert

Use case number: 011

Actor: DevOps Engineer

Use case description: This use case describes the behavior of an actor getting the alert.

Triggers: The use case is triggered when the container scan report is exported.

7. Configure notify and alert rule:

7.1 Use case name: add notify or alert rule

Use case number: 012

Actor: DevOps Engineer

Use case description: This use case describes the behavior of an actor adding a new

notification or alert rule.

Triggers: The use case is triggered when a new notification or alert rule is added.

7.2 Use case name: delete notify and alert rule

Use case number: 013

Actor: DevOps Engineer

Use case description: This use case describes the behavior of an actor deleting a notification or alert rule.

Triggers: The use case is triggered when a notification or alert rule is deleted.

7.3 Use case name: revise notify and alert rule

Use case number: 014

Actor: DevOps Engineer

Use case description: This use case describes the behavior of an actor revising a notification or alert rule.

Triggers: The use case is triggered when a notification or alert rule is revised.

8. configure vulnerability database:

8.1 Use case name: add vulnerability database

Use case number: 015

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor adding a new vulnerability database.

Triggers: The use case is triggered when a new vulnerability database is added.

8.2 Use case name: delete vulnerability database

Use case number: 016

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor deleting a vulnerability database.

Triggers: The use case is triggered when a vulnerability database is deleted.

8.3 Use case name: update vulnerability database

Use case number: 017

Actor: DevOps Engineer, Information Security Engineer, Developer

Use case description: This use case describes the behavior of an actor updating a vulnerability database.

Triggers: The use case is triggered when a vulnerability database is updated.