Integrate Docker Scout with Circle CI

The following examples runs when triggered in CircleCI. When triggered, it checks out the "docker/scout-demo-service:latest" image and tag and then uses Docker Scout to create a CVE report.

Add the following to a *.circleci/config.yml* file.

First, set up the rest of the workflow. Add the following to the YAML file:

```
version: 2.1

jobs:
  build:
    docker:
      - image: cimg/base:stable
    environment:
      IMAGE_TAG: docker/scout-demo-service:latest
```

This defines the container image the workflow uses and an environment variable for the image.

Add the following to the YAML file to define the steps for the workflow:

```
steps:
  # Checkout the repository files
  - checkout

  # Set up a separate Docker environment to run `docker` commands in
  - setup_remote_docker:
      version: 20.10.24

  # Install Docker Scout and login to Docker Hub
  - run:
      name: Install Docker Scout
      command: |
        env
```

```
        curl -sSfL https://raw.githubusercontent.com/docker/scout-cli/main/install.sh | sh -s
-- -b /home/circleci/bin
        echo $DOCKER_HUB_PAT | docker login -u $DOCKER_HUB_USER --password-stdin

  # Build the Docker image
  - run:
      name: Build Docker image
      command: docker build -t $IMAGE_TAG .

  # Run Docker Scout
  - run:
      name: Scan image for CVEs
      command: |
        docker scout cves $IMAGE_TAG --exit-code --only-severity critical,high
```

This checks out the repository files and then sets up a separate Docker environment to run commands in.

It installs Docker Scout, logs into Docker Hub, builds the Docker image, and then runs Docker Scout to generate a CVE report. It only shows critical or high-severity vulnerabilities.

Finally, add a name for the workflow and the workflow's jobs:

```
workflows:
  build-docker-image:
    jobs:
      - build
```

□□□ #2
□ □□□ □□□ 2026-10-31 19:36:55 UTC
□ □□□ □□□ 2026-10-31 19:36:56 UTC