dvnattages of Anchore

* Anchore allows you to search for Docker container images across multiple public and private registries. And, it allows you to drill down into repos to see all tags and images including image history and updates.
* Once images are discovered, you can conduct analysis on them, including searchable lists of all packages, files and software artifacts.

How Anchore Works?

Step 1 : adding an image

anchore-cli image add docker.io/library/nginx:latest

The image add command instructs the Anchore Engine to pull (download) and analyze an image from a registry.

Step 2 : Inspecting Images

anchore-cli image content INPUT\_IMAGE CONTENT\_TYPE

* Types can be :
* os: Operating System Packages
* files: All files in the image
* npm: Node.JS NPM Modules
* gem: Ruby GEMs
* java: Java Archives
* python: Python Artifacts

Step 3 : Viewing Security Vulnerabilities

anchore-cli image vuln INPUT\_IMAGE VULN\_TYPE

The INPUT\_IMAGE can be specified in one of the following formats:

* Image Digest
* Image ID
* registry/repo:tag

The VULN\_TYPE currently supports:

* os: Operating System Package CVEs
* non-os: NPM, GEM, Java Archive (jar, war, ear) and Python PIP CVEs.
* all: Combination report containing both ‘os’ and ‘non-os’ vulnerability records.