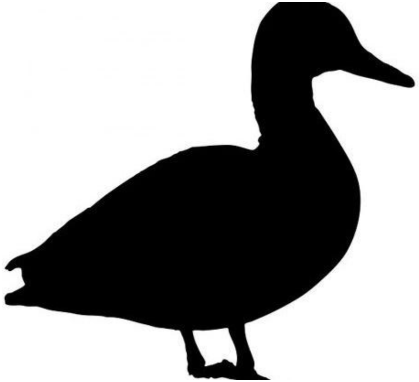
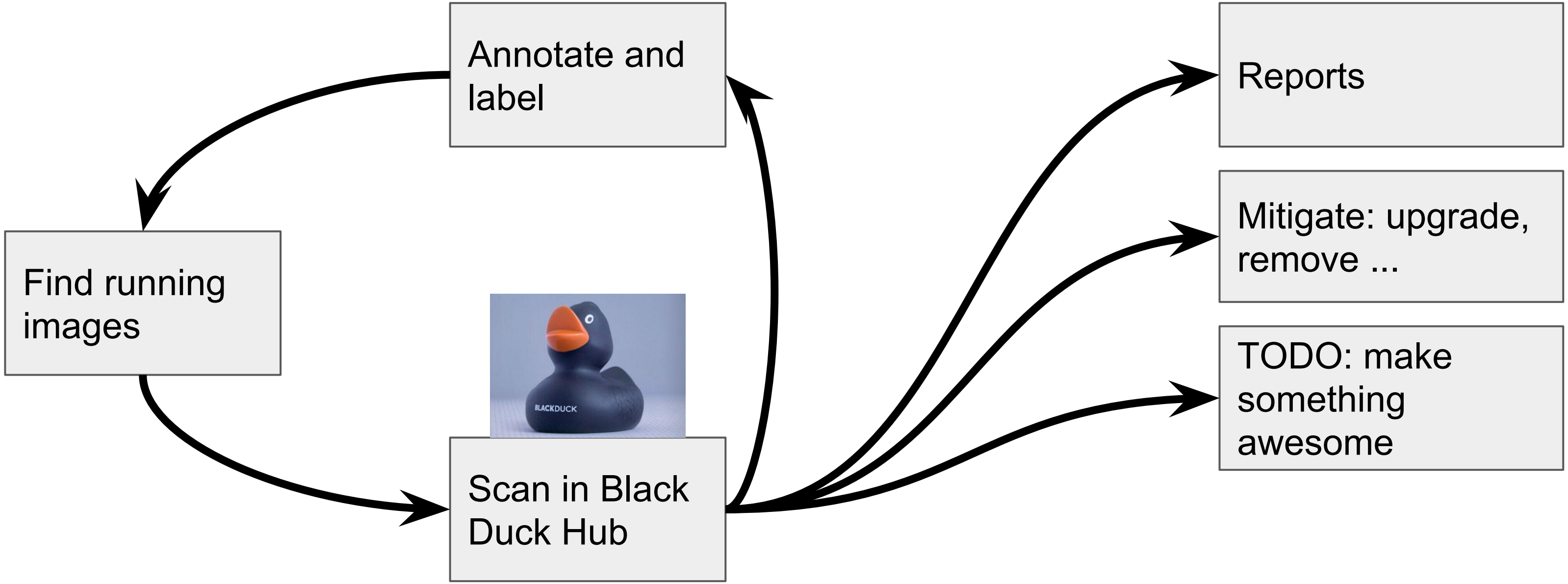
Perceptor: an open-source toolkit for cluster threat detection

Matt Fenwick



Senior Engineer, Cloud Native team
Black Duck by Synopsys

OpsSight: scan images using Black Duck Hub



Annotate and label

Find running images

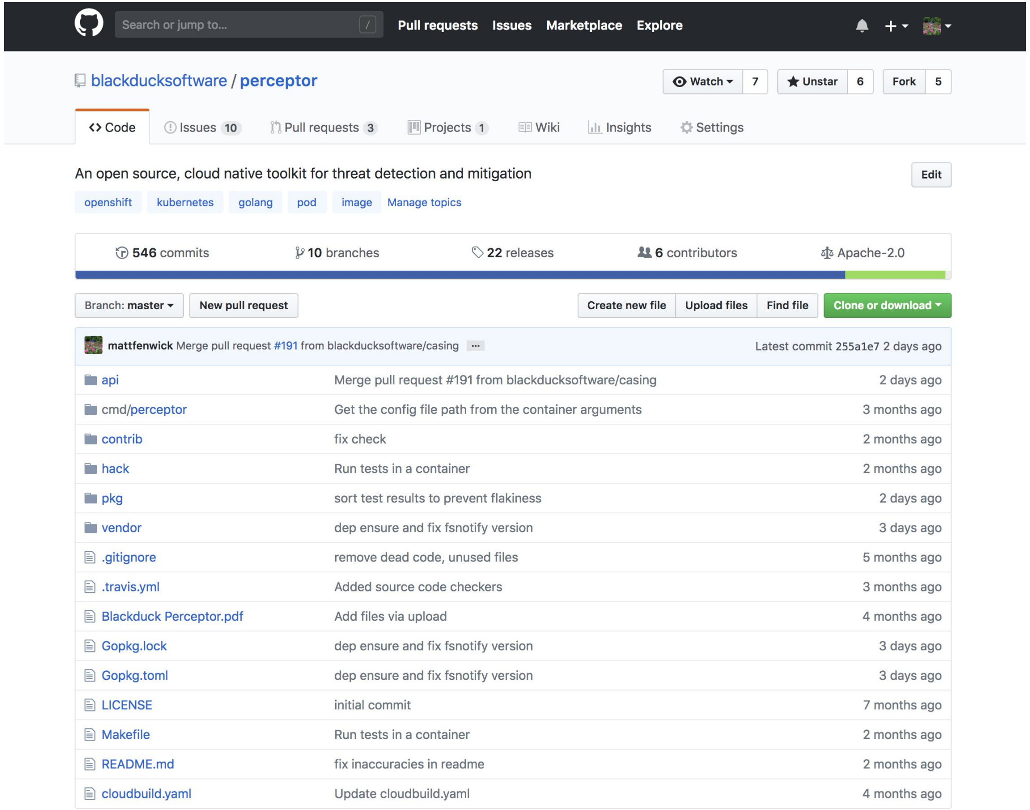
Scan in Black Duck Hub

Reports

Mitigate: upgrade, remove ...

TODO: make something awesome

github.com/blackduck/perceptor



blackducksoftware / perceptor

Watch 7 | Unstar 6 | Fork 5

<> Code | Issues 10 | Pull requests 3 | Projects 1 | Wiki | Insights | Settings

An open source, cloud native toolkit for threat detection and mitigation

Edit

openshift kubernetes golang pod image Manage topics

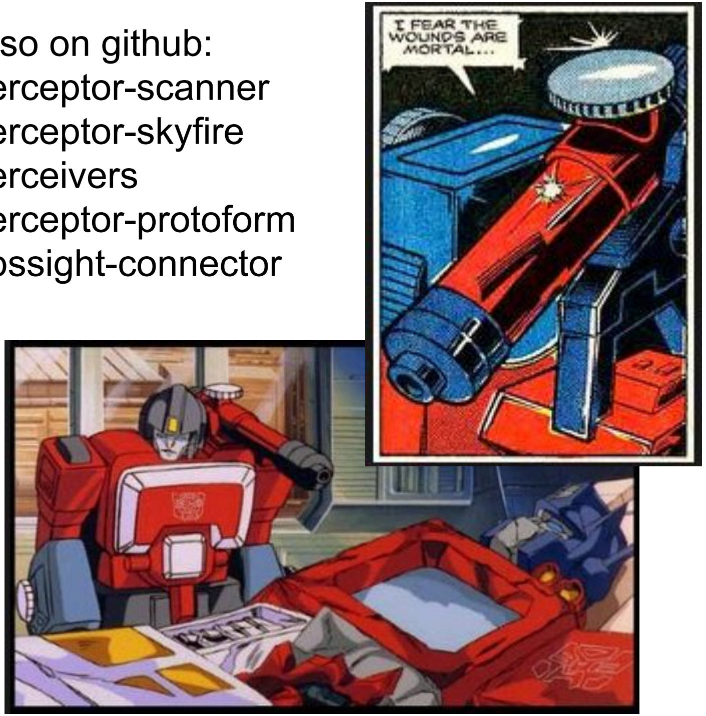
546 commits | 10 branches | 22 releases | 6 contributors | Apache-2.0

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

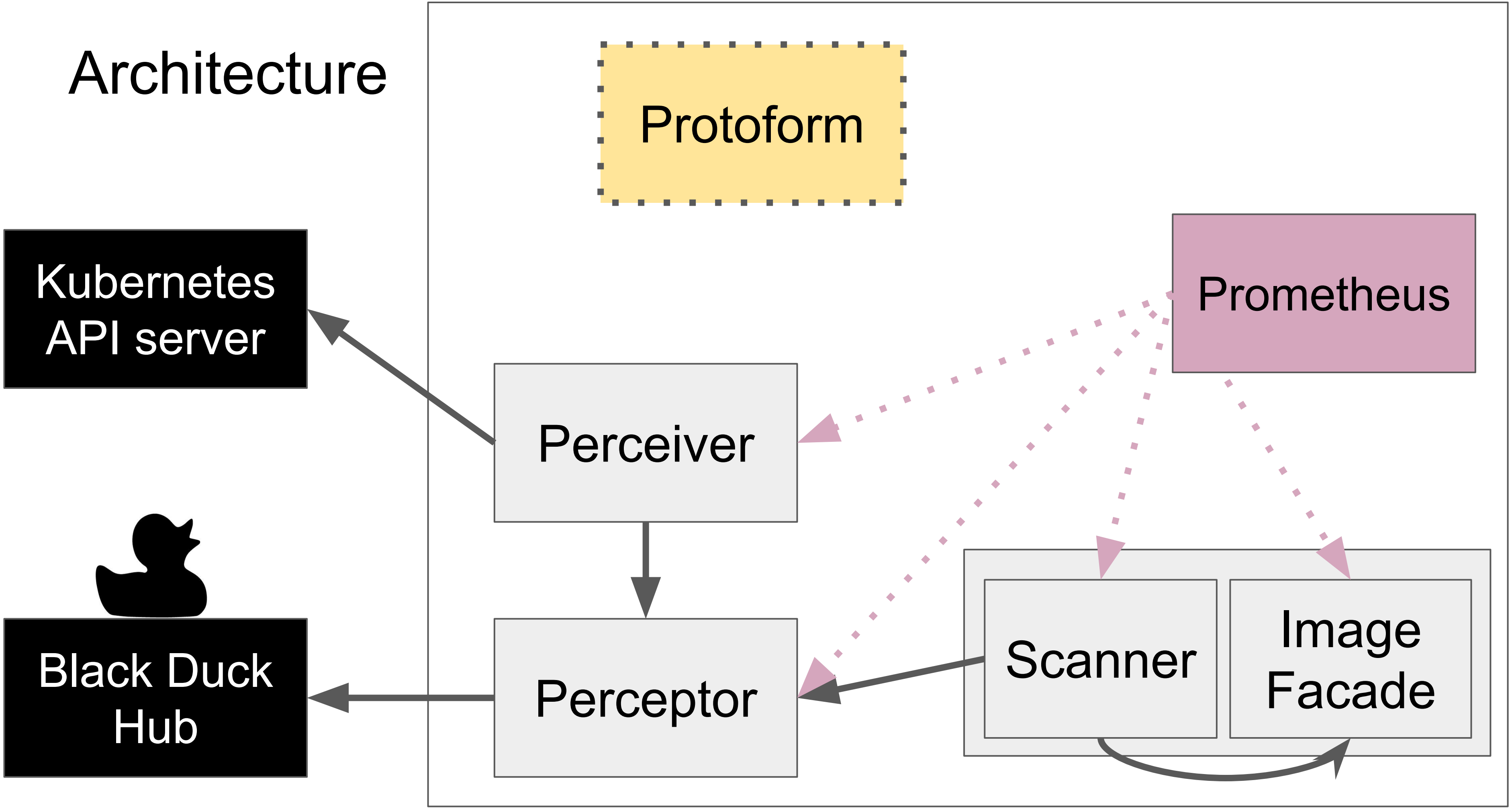
mattfenwick Merge pull request #191 from blackducksoftware/casing ... Latest commit 255a1e7 2 days ago

api	Merge pull request #191 from blackducksoftware/casing	2 days ago
cmd/perceptor	Get the config file path from the container arguments	3 months ago
contrib	fix check	2 months ago
hack	Run tests in a container	2 months ago
pkg	sort test results to prevent flakiness	2 days ago
vendor	dep ensure and fix fsnotify version	3 days ago
.gitignore	remove dead code, unused files	5 months ago
.travis.yml	Added source code checkers	3 months ago
Blackduck Perceptor.pdf	Add files via upload	4 months ago
Gopkg.lock	dep ensure and fix fsnotify version	3 days ago
Gopkg.toml	dep ensure and fix fsnotify version	3 days ago
LICENSE	initial commit	7 months ago
Makefile	Run tests in a container	2 months ago
README.md	fix inaccuracies in readme	2 months ago
cloudbuild.yaml	Update cloudbuild.yaml	4 months ago

Also on github:
perceptor-scanner
perceptor-skyfire
perceivers
perceptor-protoform
opssight-connector



Architecture



Protoform

Kubernetes API server

Prometheus

Perceiver

Black Duck Hub

Perceptor

Scanner

Image Facade

Perceptor core

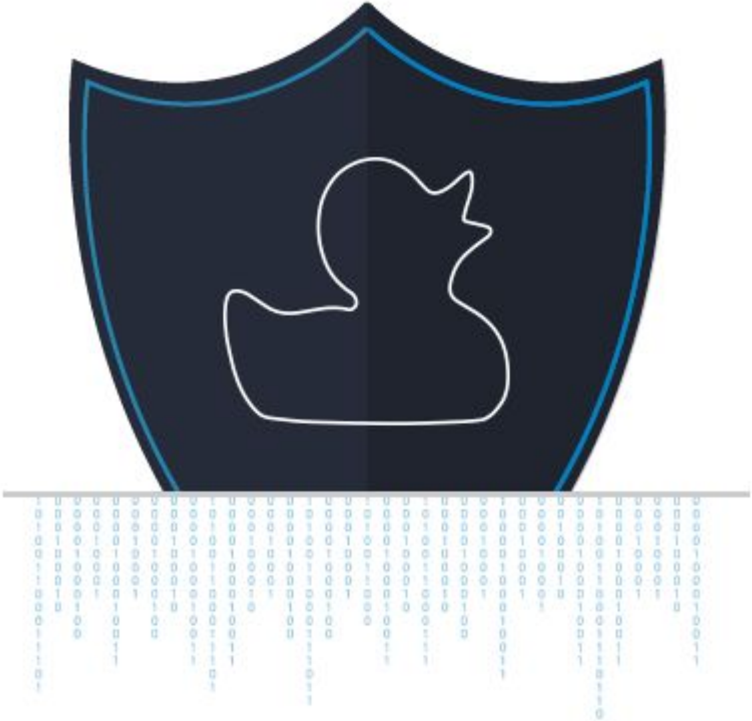
Model

Code structure

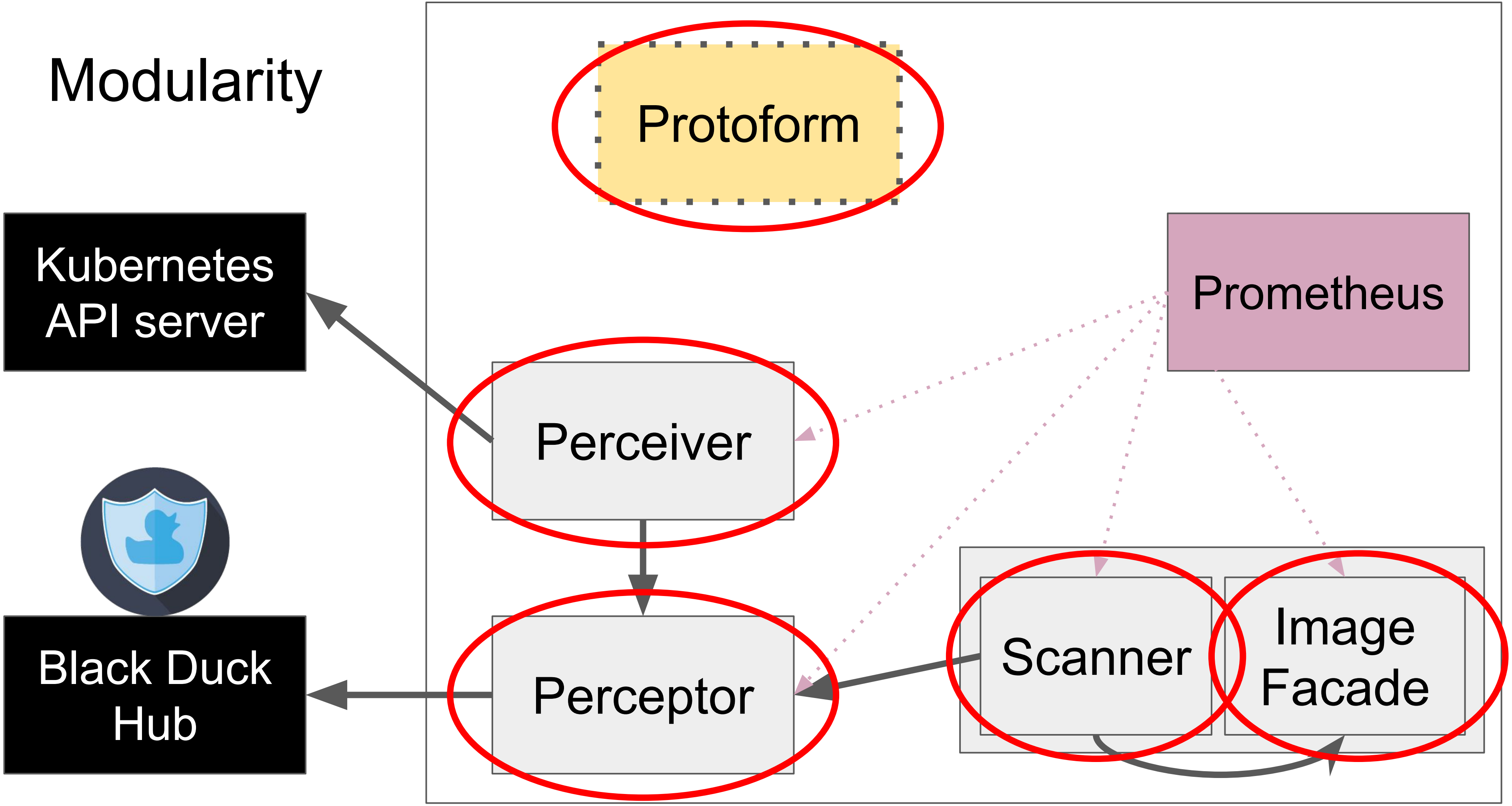
Metrics

Protoform

Skyfire



Modularity


Protoform
Kubernetes API server
Prometheus
Perceiver
Black Duck Hub
Perceptor
Scanner
Image Facade

Challenges

Scaling!

Kube limits as of 1.11:

- 5000 nodes
- 150000 pods
- 300000 containers
- 100 pods per node

Acknowledgements

Senthil Manikantan
Rob Rati
Jay Vyas
Tim Mackey
Jonathan Beakley
Neal Goldman
Joel Sheppard
Dave Meurer

blackduck™

Conclusion

Cluster threat management in real time.

Open source! Collaborations welcome!

Fun TODOs!

- more scan technologies
- different types of scanning (layer, containers)
- more Kubernetes features (admission controllers)
- more container orchestrators (Docker compose, Docker swarm)
- more container runtimes (crio)

SYNOPSYS®