



Container Security Scanning for Vulnerabilities

Roberto Soares (Speaker)

Ricardo Rocha (Supervisor)

2018

CERN Cloud

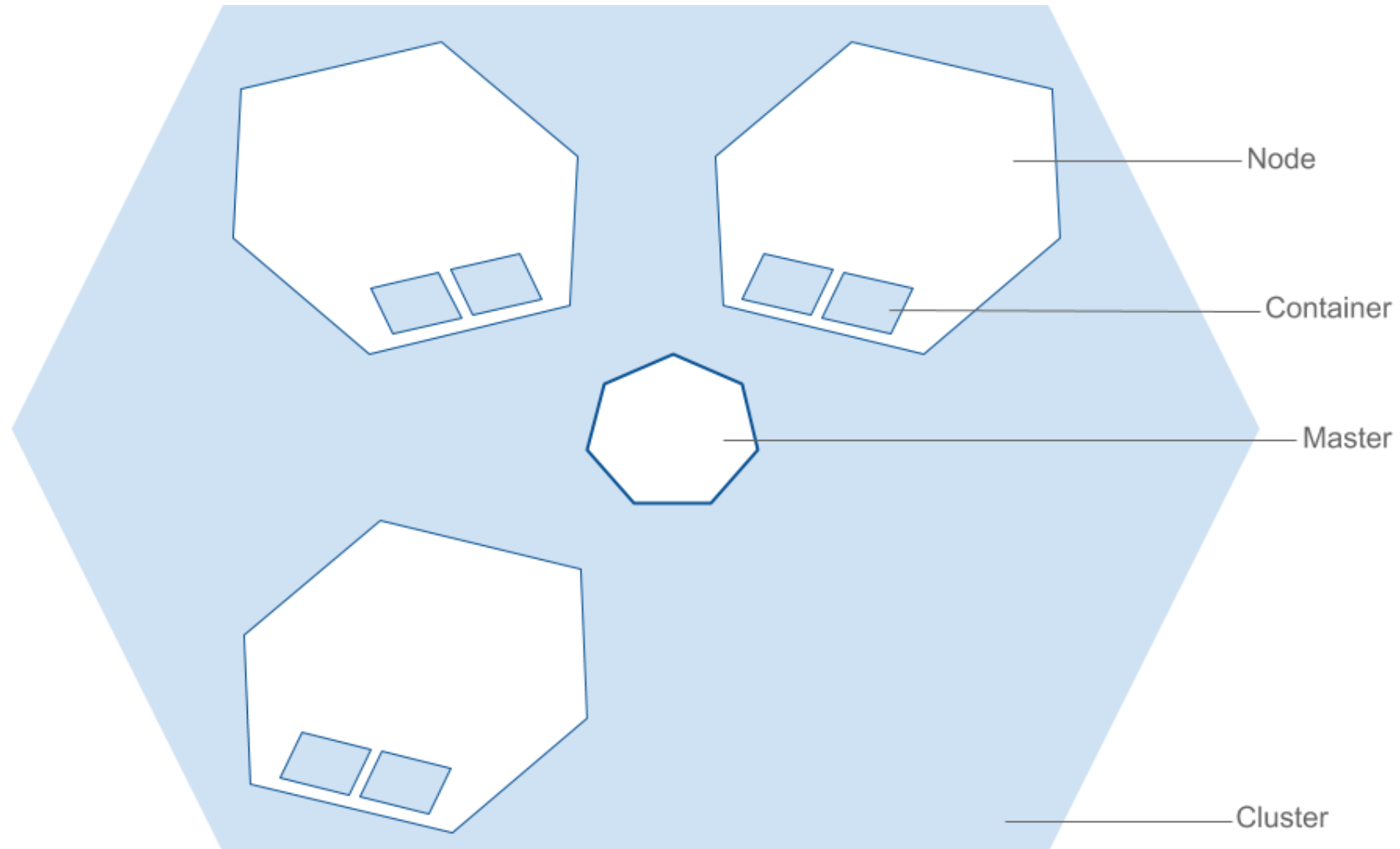
Introduction

- Cloud management software
- Virtual machines on demand... and clusters



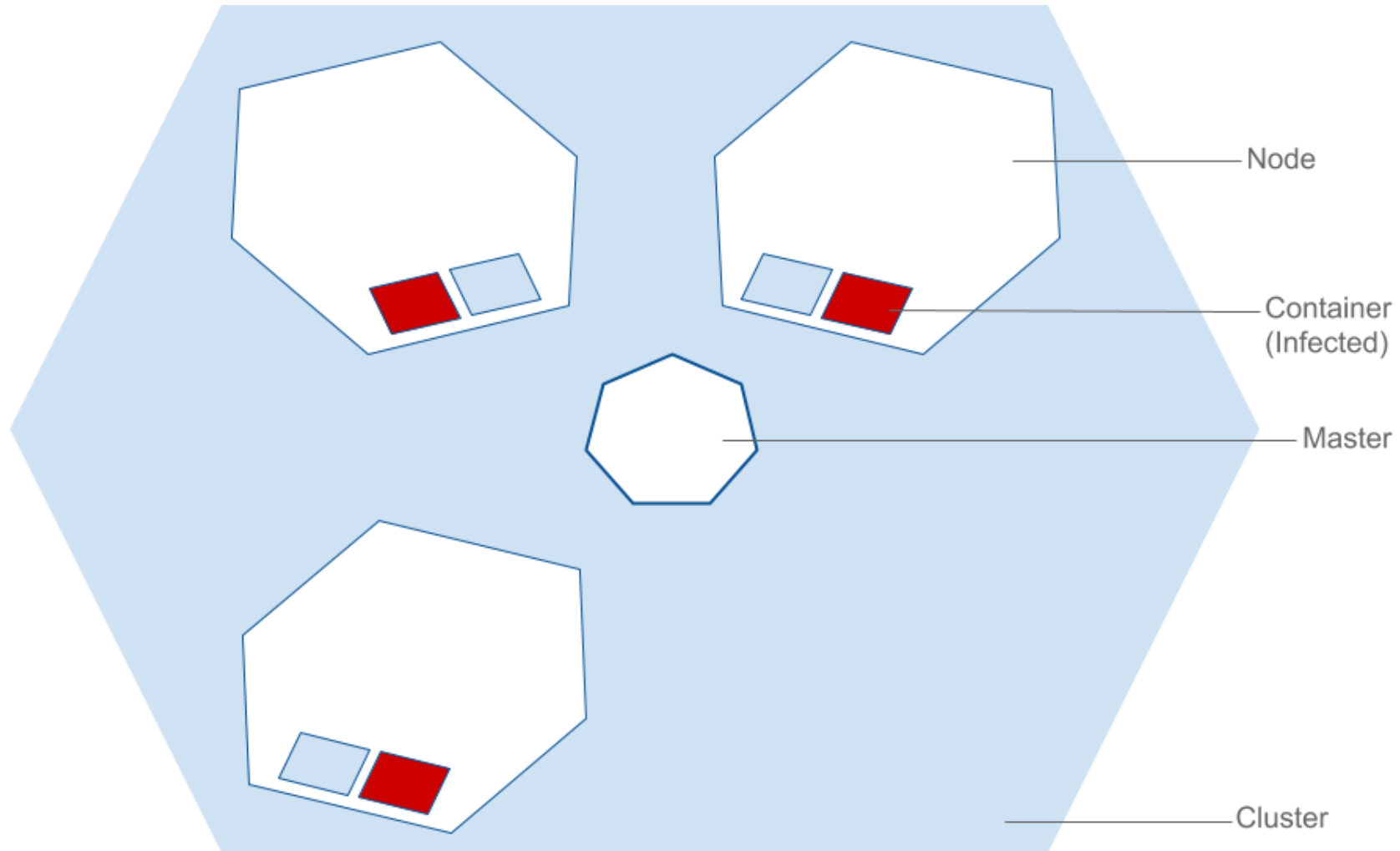
Kubernetes

Introduction



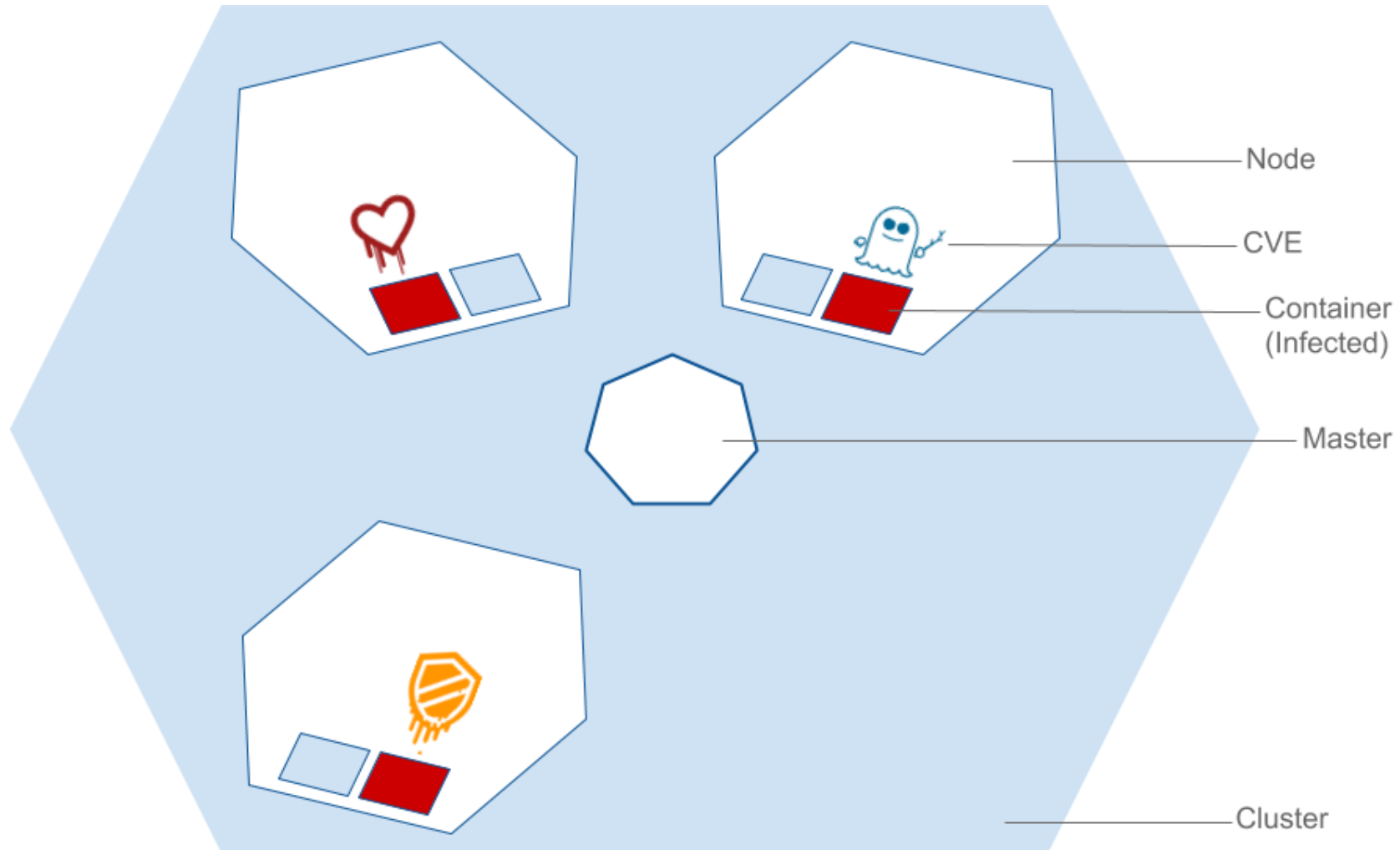
Security

Motivation



Security

Problem Statement



<http://cern.ch/go/8tdg>

<http://cern.ch/go/Q67r>

<http://cern.ch/go/x8Vq>

CoreOS Clair

Solution

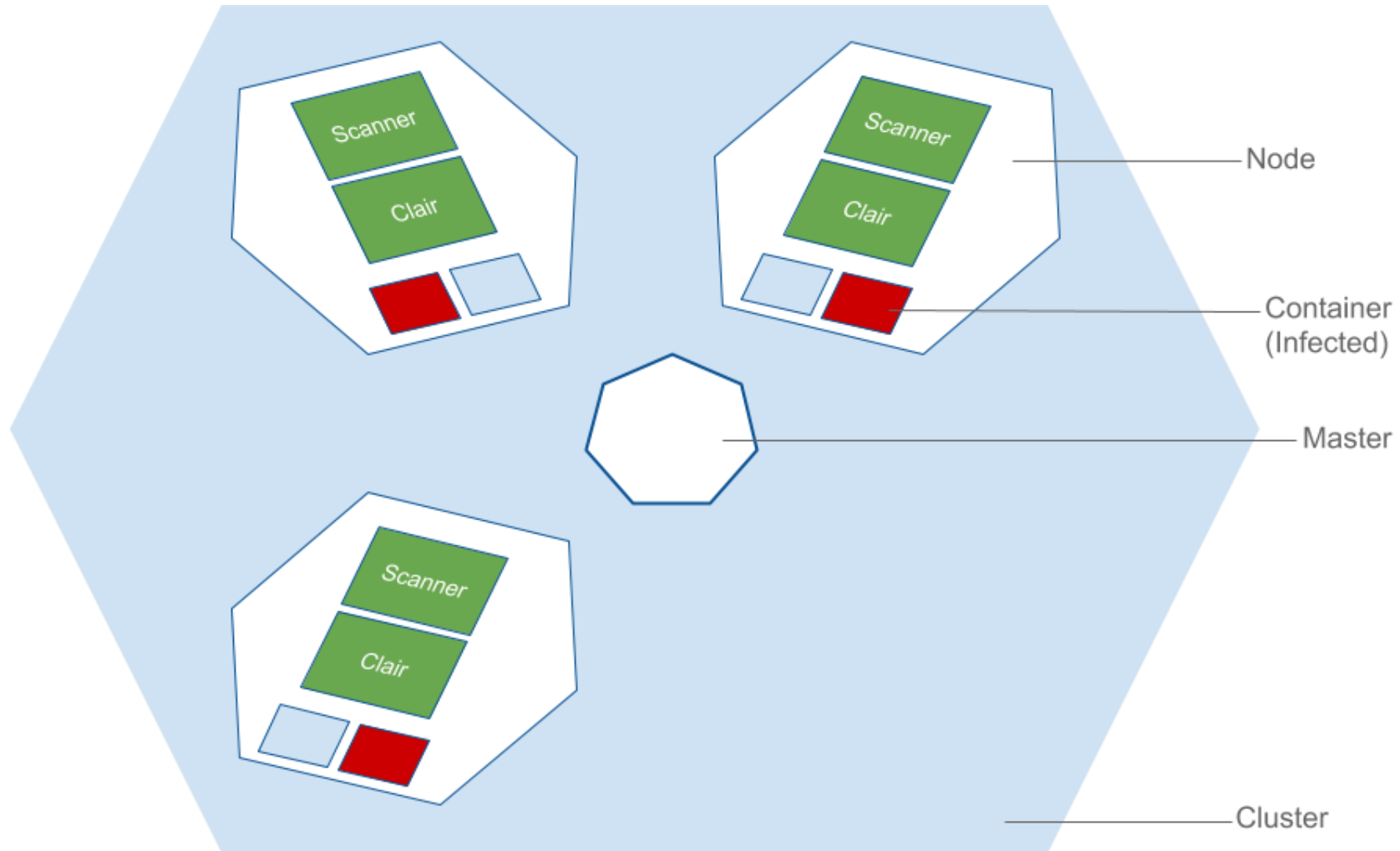
- Static analysis of vulnerabilities in containers
- Alert users



clair

Scanner

Solution



Scanner

Results

```
2018-08-08 19:29:35,224 INFO root - Starting scan...
2018-08-08 19:29:59,810 INFO root - Marking pod dvwa-5bb6cd9987-8nz87 as vulnerable. A total of 137 vulnerabilities were found.
2018-08-08 19:29:59,810 INFO root - Image docker.io/vulnerables/web-dvwa@sha256:ab131e6c0fd8c3319ce0f5e7c
db551102587cad9ba50b18fd468584b00d0767d has 137 vulnerabilities.
2018-08-08 19:30:29,314 INFO root - Marking pod gangly-starfish-clair-f79b9d587-8z9q5 as safe. 0 vulnerabilities found on all containers.
2018-08-08 19:30:49,666 INFO root - Marking pod gangly-starfish-postgresql-67dccfbf89-h6q7j as vulnerable. A total of 93 vulnerabilities were found.
2018-08-08 19:30:49,667 INFO root - Image docker.io/postgres@sha256:5284ba74a1065e34cf1bfccd64caf8c497c8dc623d6207b060b5ebd369427d34 has 93 vulnerabilities.
2018-08-08 19:31:07,353 INFO root - Marking pod gangly-starfish-vulnerability-scanner-bzdtt as safe. 0 vulnerabilities found on all containers.
2018-08-08 19:31:31,627 INFO root - Marking pod csi-cephfsplugin-kcfkv as vulnerable. A total of 7 vulnerabilities were found.
2018-08-08 19:31:31,628 INFO root - Image gitlab-registry.cern.ch/cloud/atomic-system-containers/cephfsplugin@sha256:169f2608a6f5d1cc3d3f13454e0b32f4ff4ca6bc8371737ba799568c2c7da3b7 has 7 vulnerabilities.
2018-08-08 19:31:31,630 INFO root - Image gitlab-registry.cern.ch/cloud/atomic-system-containers/driver-registry@sha256:06d30df6397491e98be9d772fa2d4abc840761b9861eba88fd38799f594a69ec has 0 vulnerabilities.
2018-08-08 19:31:55,607 INFO root - Marking pod csi-cvmfsplugin-p6t66 as safe. 0 vulnerabilities found on all containers.
2018-08-08 19:31:57,593 INFO root - Marking pod tiller-deploy-759cb9df9-4xdxs as safe. 0 vulnerabilities found on all containers.
2018-08-08 19:31:57,604 INFO root - Scan finished.
```


Scanner

Project Status

- ✓ Scanner working with CoreOS Clair
- ✓ Deployed on a Kubernetes cluster
- ✓ Contributed to Clair upstream

Scanner

Future Work

- ✓ Scanner working with CoreOS Clair
- ✓ Deployed on a Kubernetes cluster
- ✓ Contributed to Clair upstream
- Push it to OpenStack Magnum upstream
- More features for the scanner



Questions?

roberto.soares@cern.ch