Hacking Kubernetes And protecting yourself against it

Bastian Hofmann

Agenda

01
- Introduction: Container and Kubernetes Security

02
- Ad hack that will us allow to take over a web app in a Kubernetes cluster

03
- Secure our cluster to protect against this and other attacks

What I do

What is Qdrant?

Qdrant is a vector similarity search engine (or vector database)

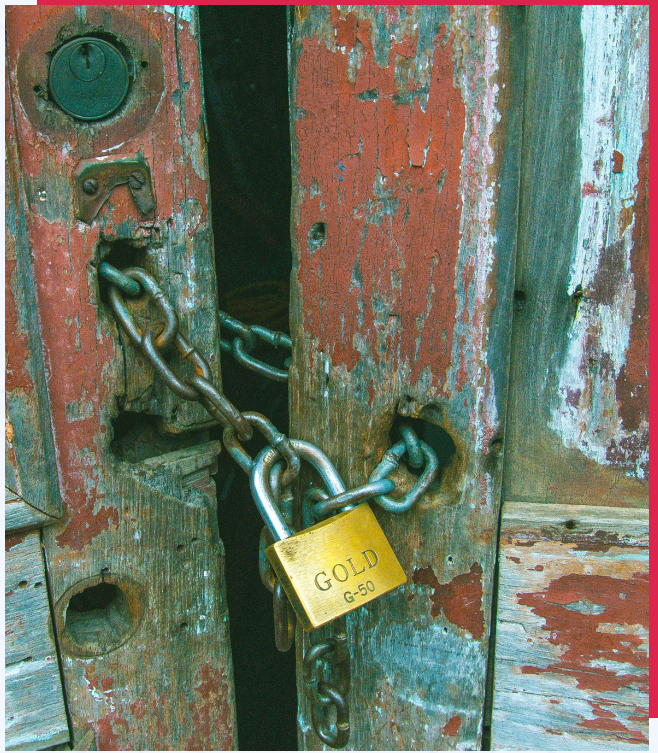
- Semantic search
- Recommendations
- Fraud detection
- Anomaly detection
- Generative AI
- ...

Thanks to

Nico Meisenzahl
(https://github.com/nmeisenzahl)
Koz (https://github.com/kozmer)
For inspiration and PoC app

kubernetes

Security



The Kubernetes Cluster

KUBERNETES / SECURITY / CONTRIBUTED

Kubernetes Is a High-Value Cyberwar Target

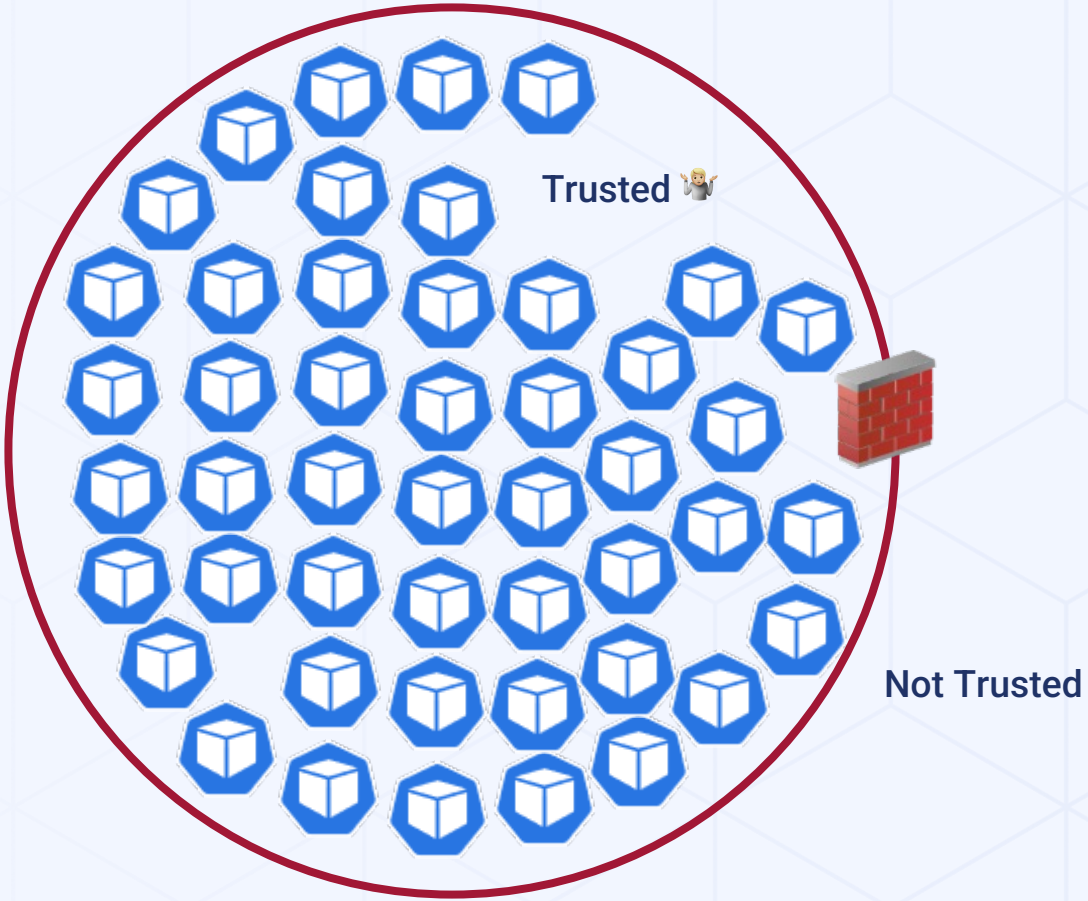
9 Mar 2022 10:00am, by Michael Clark

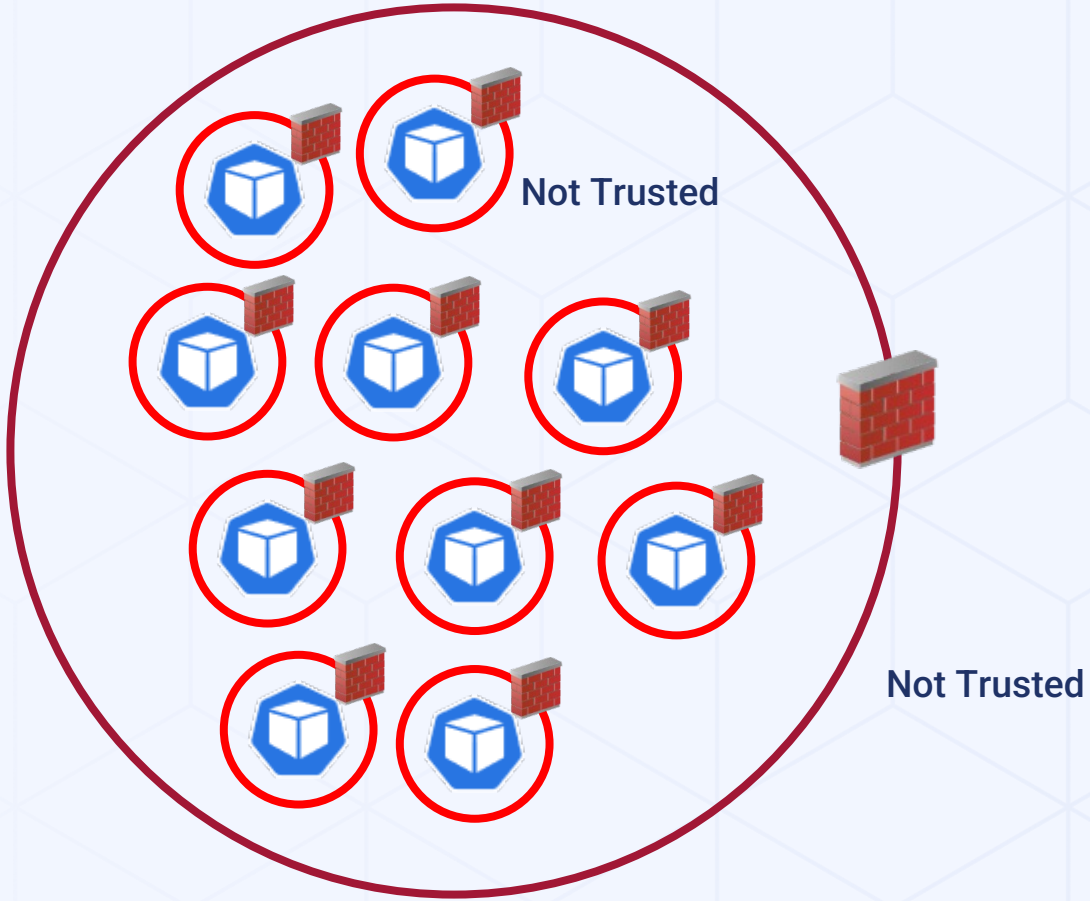
Kubernetes Cluster

Security Considerations

- API access
- RBAC
- Certificate management
- Version upgrades
- Admission Control
- Security Policies
- Etcd Encryption
- Network Policies
- Traffic encryption

Your application


Trusted
Not Trusted

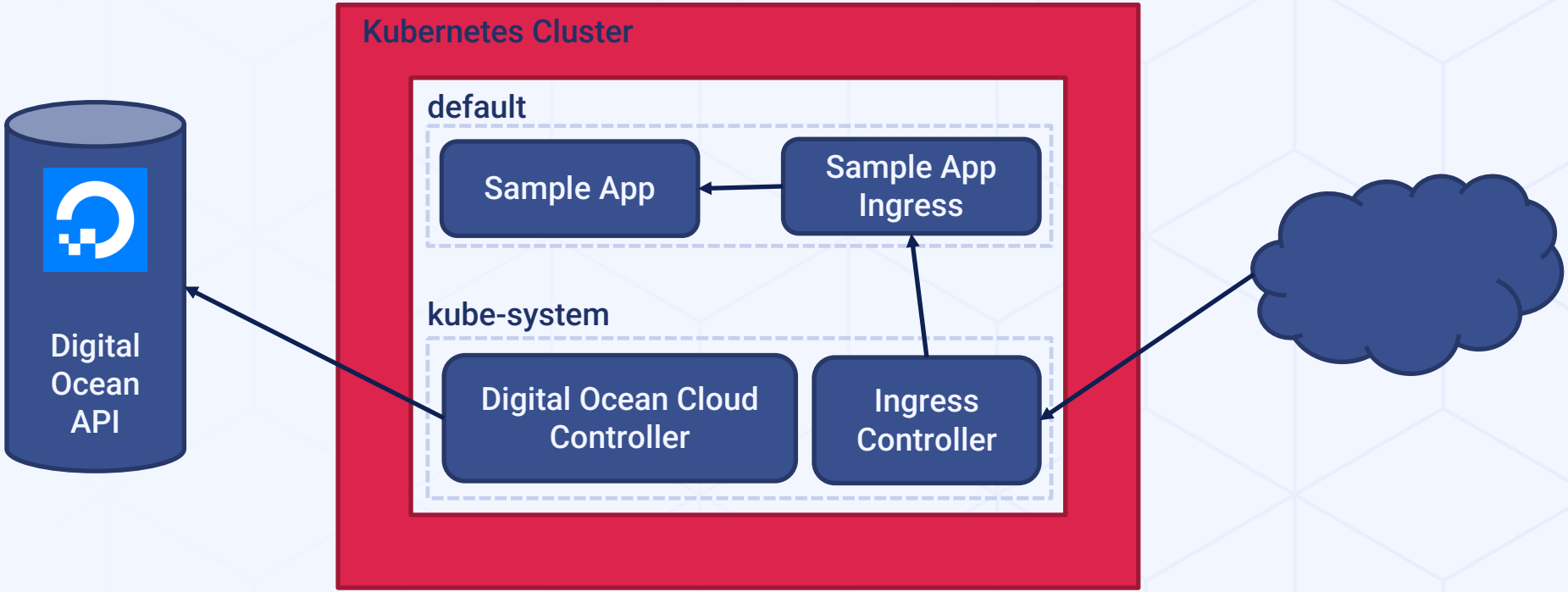

Not Trusted
Not Trusted

Containerized Application

Security Considerations

- Container capabilities
- Compliance issues
- CVEs in base images
- CVEs in installed packages
- CVEs in frameworks and other libraries
- Bugs in software

Demo Application

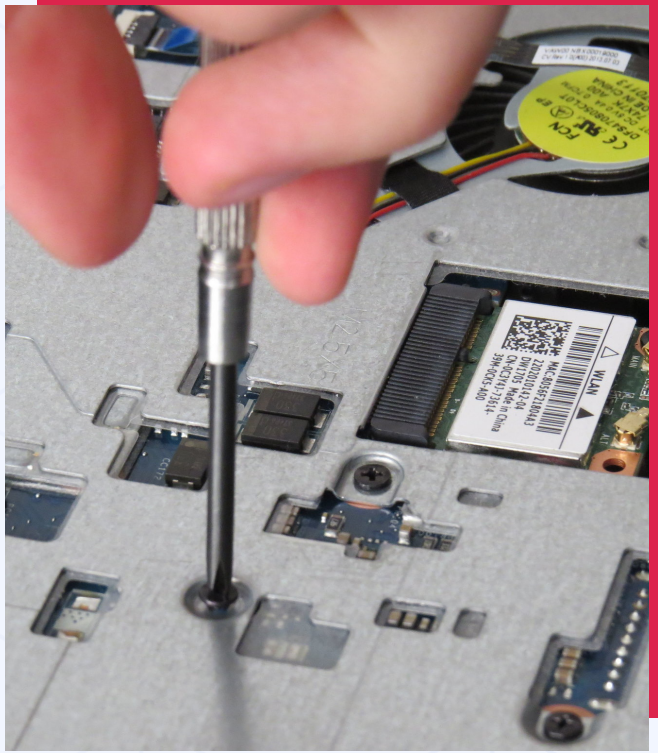


Let‘s hack into it

What did just happen?

- The sample app had a Log4Shell vulnerability
- The attacker was able to exploit it and get a remote shell into the sample app container
- They could modify the file system of the container
- They could escape the container and get SYS_ADMIN capabilities
- They could create a remote shell as root directly on the host
- They could get an admin kubeconfig of the Kubernetes cluster
- They could read out the cloud-credential Secret in the kube-system namespace with a DigitalOcean API token
- They could take over the DigitalOcean account and create VMs

Let‘s fix it

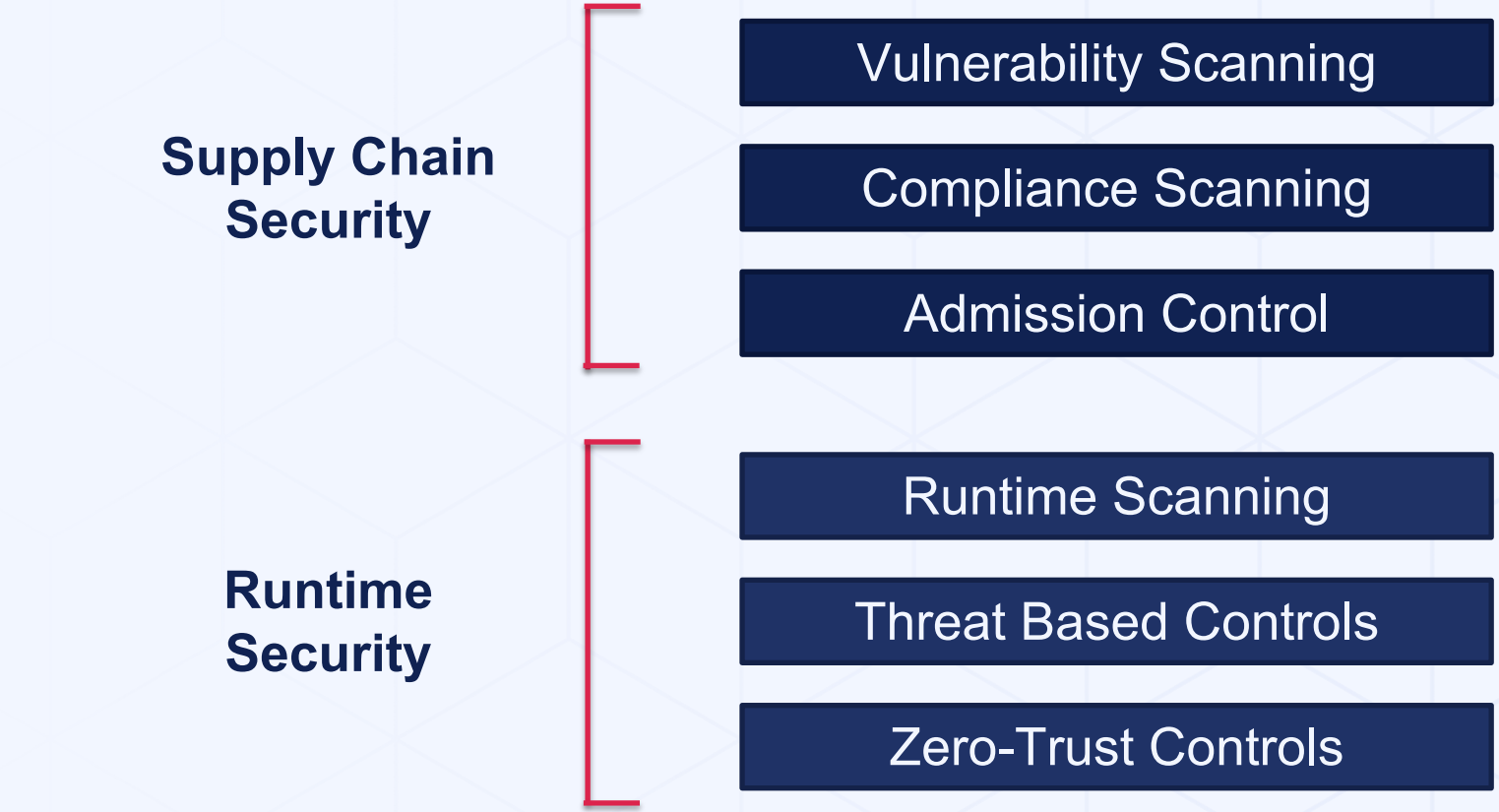


NeuVector

- Limit the capabilities of containers and prevent the deployment of insecure images

Scanning images is important

Scanning images is not enough


Supply Chain Security
Vulnerability Scanning
Compliance Scanning
Admission Control
Runtime Security
Runtime Scanning
Threat Based Controls
Zero-Trust Controls

Runtime Behavioral Inspection

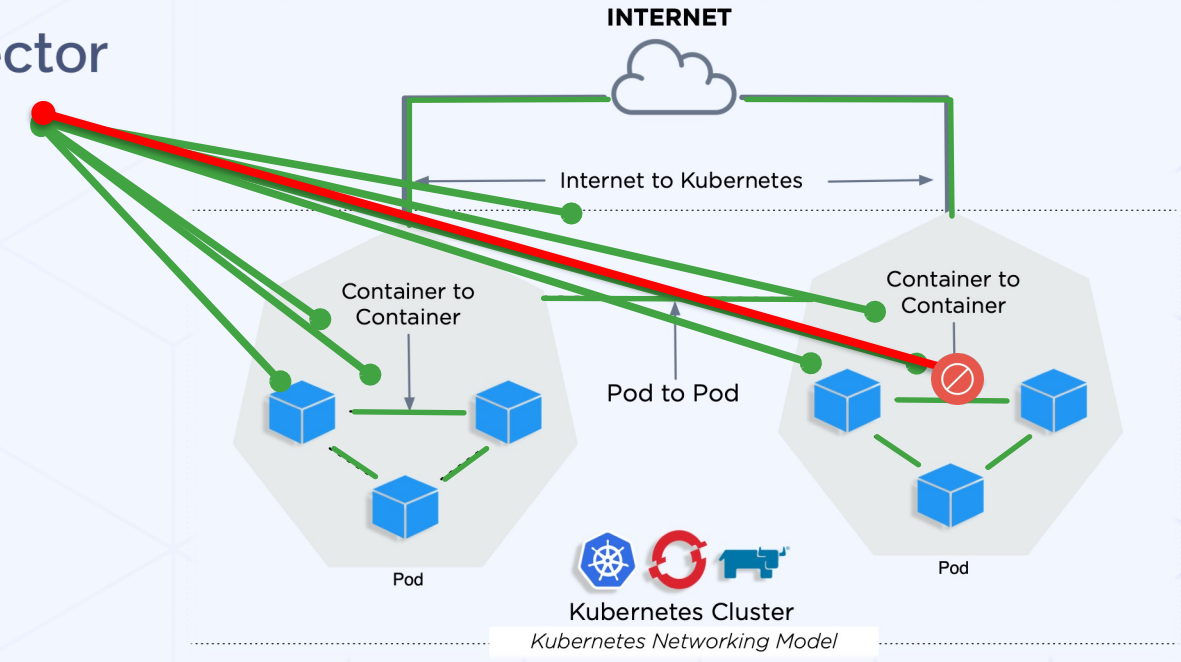
NeuVector

K8's Deep Packet Inspection

- Layer 3/4 Port
- Layer 7 Protocol
- WAF

+

- Processes



Demo

Resources

- https://www.kubewarden.io/
- https://neuvector.com/
- https://github.com/bashofmann/hacking-kubernetes

Thank you

Bastian.Hofmann@qdrant.com

Picture credits

https://flickr.com/photos/befuddledsenses/
https://flickr.com/photos/apolosales/
https://flickr.com/photos/craigsd/
https://flickr.com/photos/rjs-yes/
https://flickr.com/photos/136770128@N07/