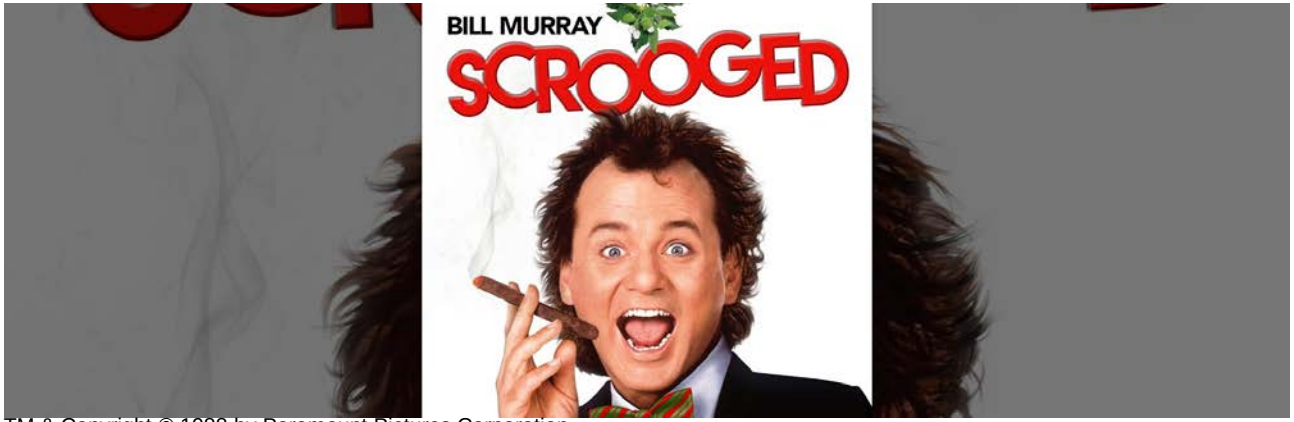
Controlware Security Day 2022

Die Container, die ich rief

Tobias Babin, Controlware GmbH, Lead Cloud Consultant

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau



Die Container, die ich rief

Tobias Babin, Controlware GmbH, Lead Cloud Consultant

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau

Agenda

controlware

1

Die Welt der Container

2

Böse Geister

3

Gute Geister

Disclaimer

controlware

Keine Produktnennung oder -empfehlung.

Fokus auf Kubernetes als Container Plattform

(Fast) nichts über Firewalls

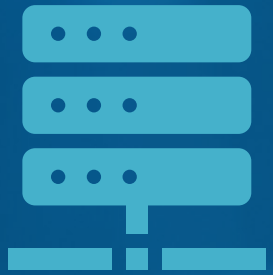
1

Die Welt der Container

Berühmte letzte Worte

"Ich hab diese Appliance gefunden, die tut genau das, was wir brauchen.

Ich muss sie nur noch in unser internes Netzwerk hängen und einschalten."



"Ich hab dieses Container Image gefunden, das tut genau das, was wir brauchen.

Ich muss es nur noch auf unseren Cluster deployen."

Alles ganz einfach

controlware

```
$ docker run my-fabulous-image
```

```
$ kubectl run fabulous --image=my-fabulous-image
```

```
$ helm install fabulous my-fabulous-chart
```

Alles ganz einfach

controlware

Portabel

("portable")

Autark

("self sufficient")

Skalierbar

("scalable")

Haben wir da ein Problem?

controlware

96% der Organisationen…

…benutzen oder evaluieren Container Technologien.[1]

89% der CISOs…

…sagen: "Microservices, Container und Kubernetes haben blinde Flecken in der Anwendungssicherheit erzeugt." [2]

97% der Organisationen…

…haben keinen Echtzeit-Einblick zu Laufzeit-Vulnerabilities in container-basierten Produktionsumgebungen. [2]

63% der CISOs…

…sagen: "DevOps und agile Entwicklung haben es schwieriger gemacht, Software Vulnerabilities zu erkennen und zu managen." [2]

[1] CNCF 2021 Cloud Native Survey (https://www.cncf.io/announcements/2022/02/10/cncf-sees-record-kubernetes-and-container-adoption-in-2021-cloud-native-survey/

[2] 2021 CISO Report (https://www.dynatrace.com/info/cloud-application-security-ciso-research/)

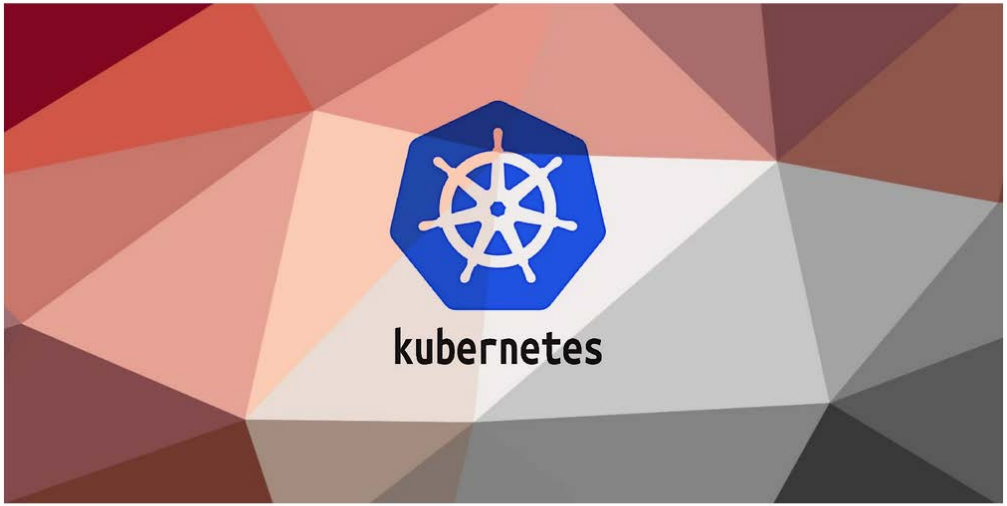
Haben wir da ein Problem?

controlware

Over 900,000 Kubernetes instances found exposed online

By Bill Toulas

June 28, 2022 06:39 AM



Over 900,000 misconfigured Kubernetes clusters were found exposed on the internet to potentially malicious scans, some even vulnerable to data-exposing cyberattacks.

https://www.bleepingcomputer.com/news/security/over-900-000-kubernetes-instances-found-exposed-online/amp/

Ein Container Image entsteht

controlware

MyApp

</>

DOCKERFILE

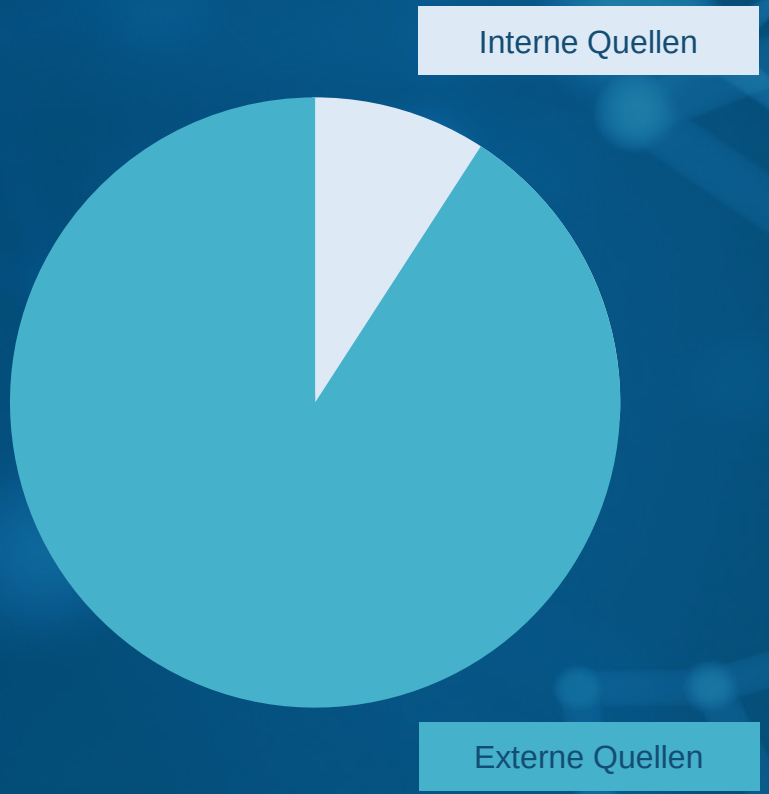
```
FROM python:3.8-slim

RUN apt-get update -y \
    && apt-get install libsasl2-dev...

COPY myscripts .

COPY requirements.txt requirements.txt
RUN pip install -r requirements.txt
```

Container Image "MyApp"

- Code Dependencies
- App </>
- Extra Libs
- Base Image
  - Libs/Bins
  - Base Image des Base Image
    - Libs/Bins
    - OS Anteile

Ein Container Image entsteht

controlware

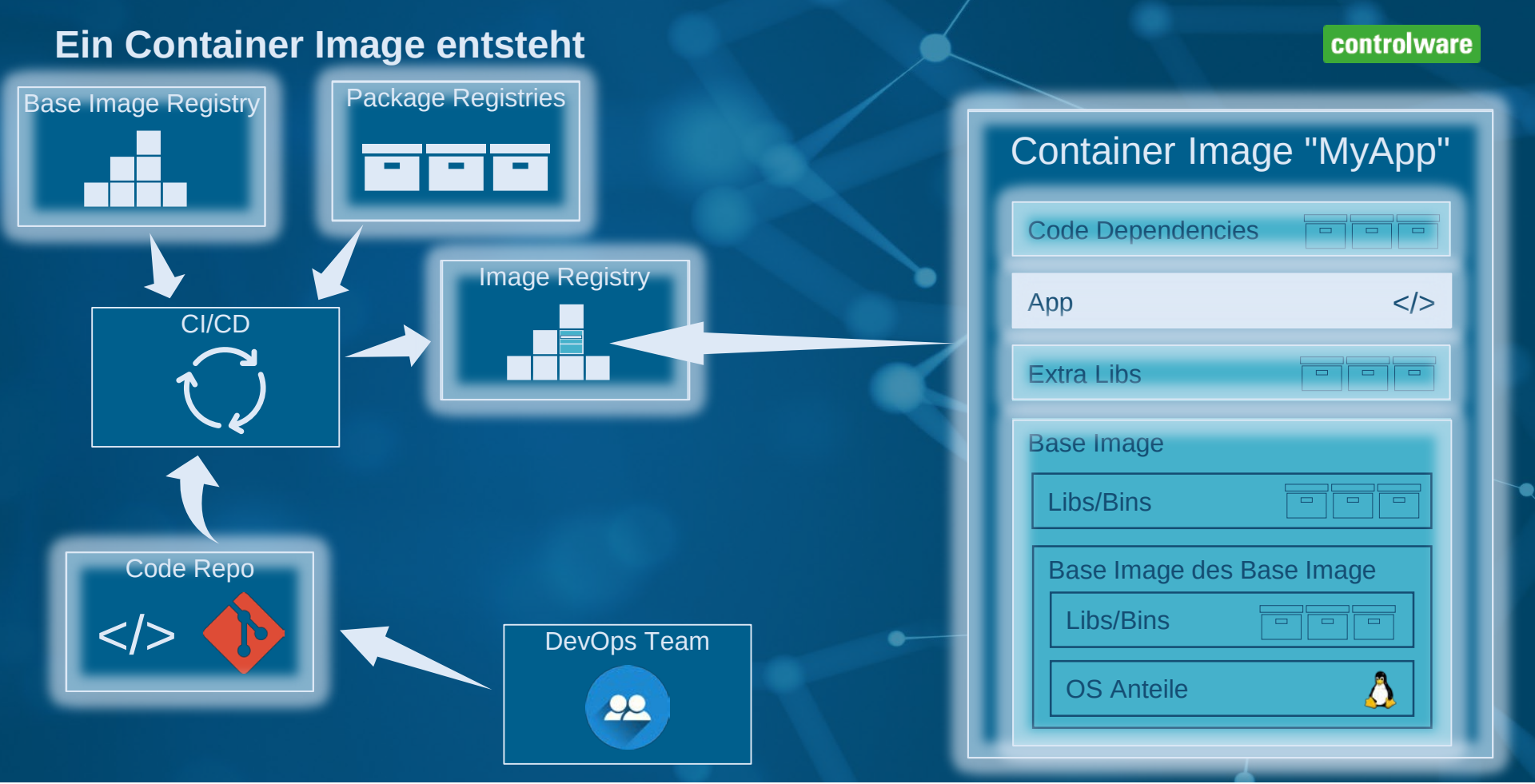


Container Image "MyApp"

- Code Dependencies
- App </>
- Extra Libs
- Base Image
  - Libs/Bins
  - Base Image des Base Image
    - Libs/Bins
    - OS Anteile

Ein Container Image entsteht

controlware



Der Container, den ich rief

controlware

Base Image Registry

Package Registries

Image Registry

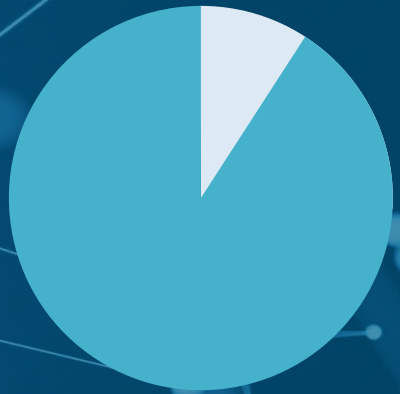
CI/CD

Container Runtime

Code Repo

DevOps Team

Interne Quellen



Externe Quellen

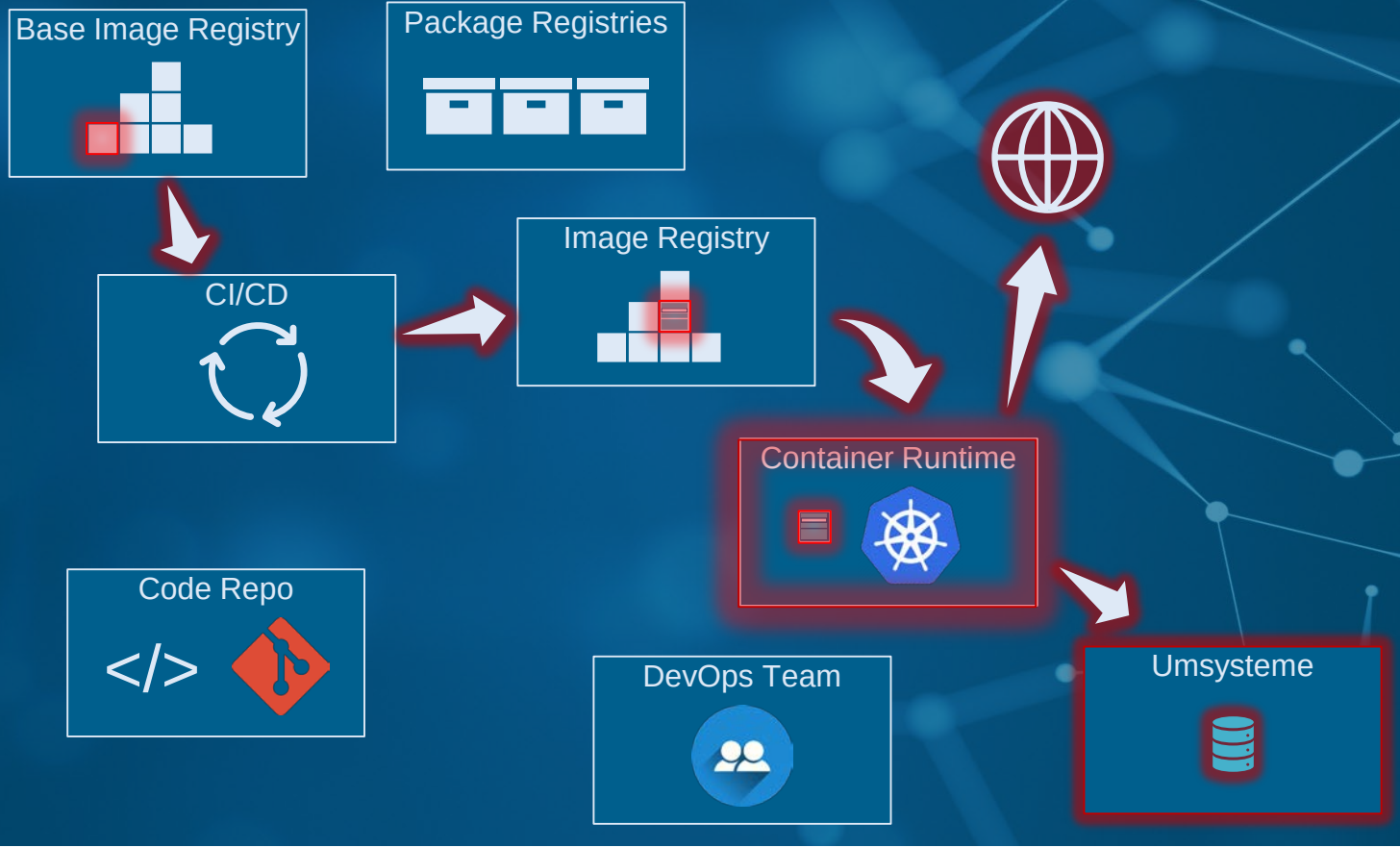
Böse Geister

controlware

Poisoned Images

Poisoned Images

controlware



Böse Geister

controlware

Sidecar Injection

Sidecar Injection

controlware

Base Image Registry

Package Registries

Image Registry

CI/CD

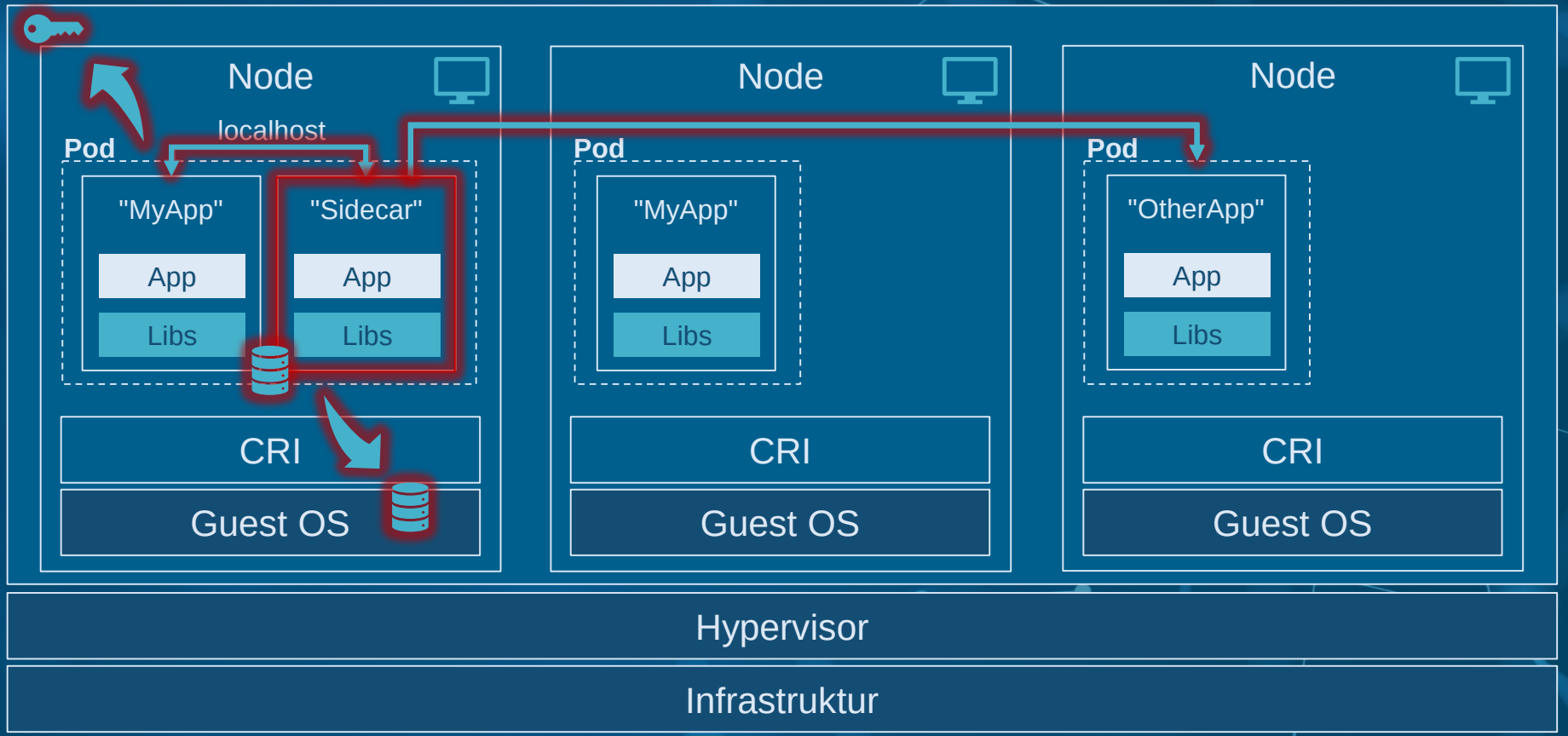
Code Repo

</>

DevOps Team

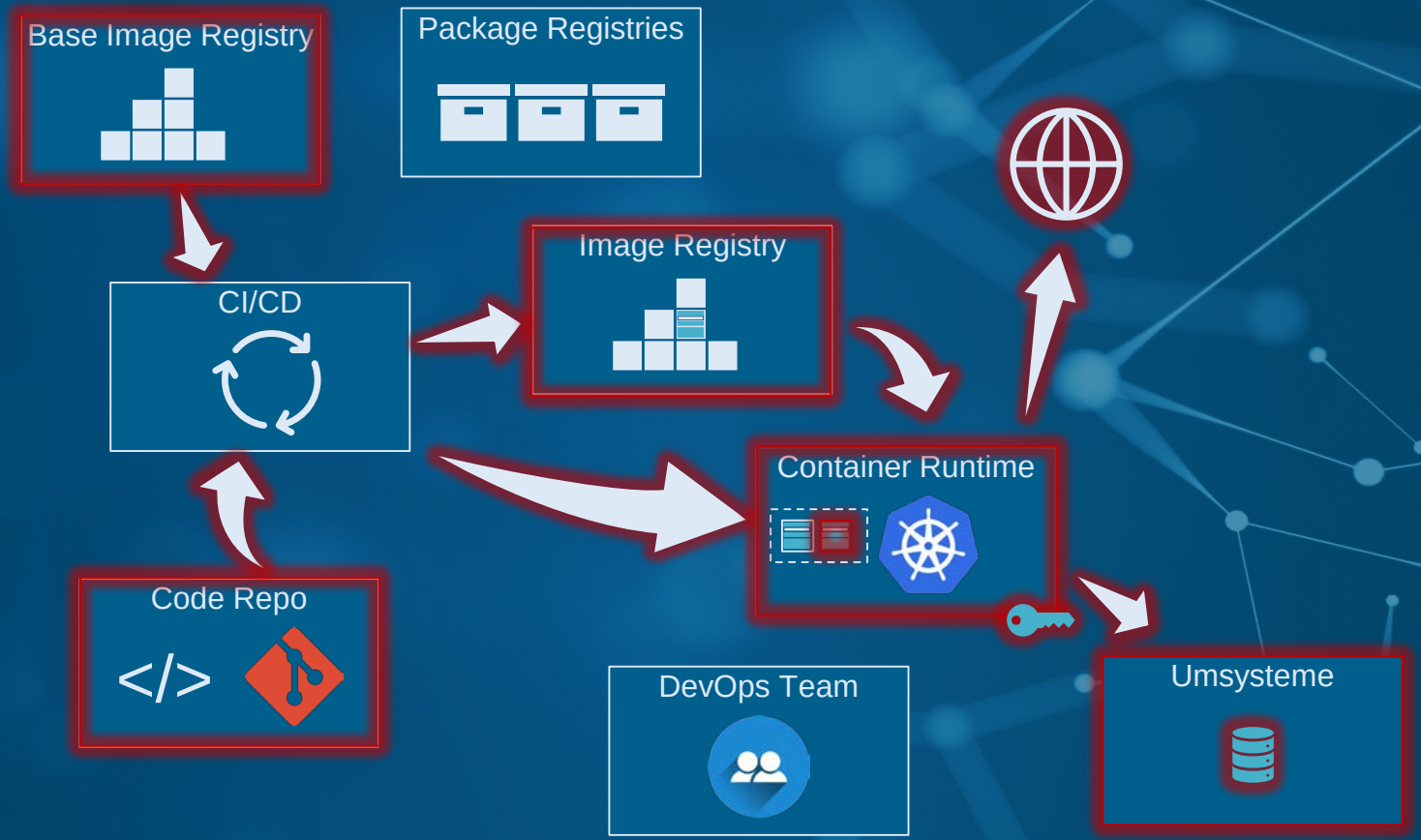
Sidecar Injection

Sidecar Injection



Sidecar Injection

controlware

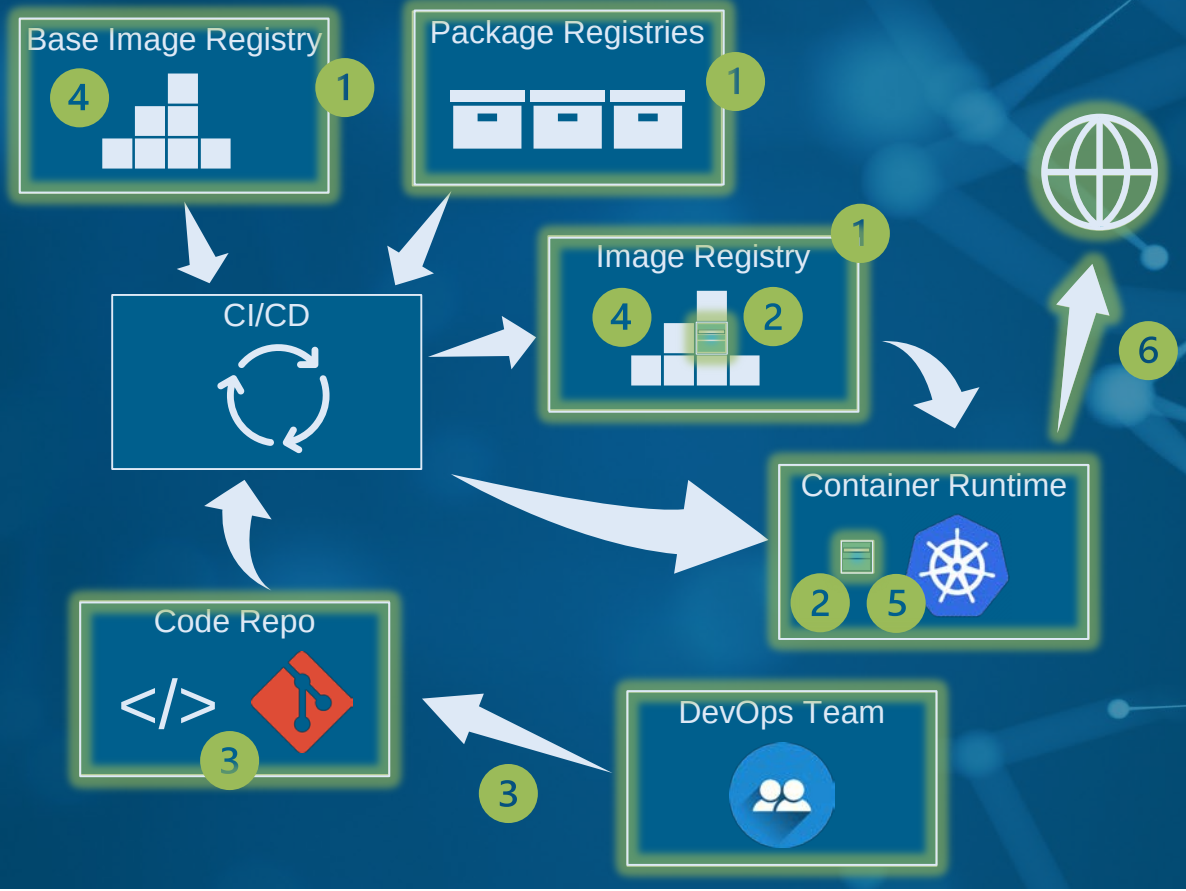


3

Gute Geister

Gute Geister

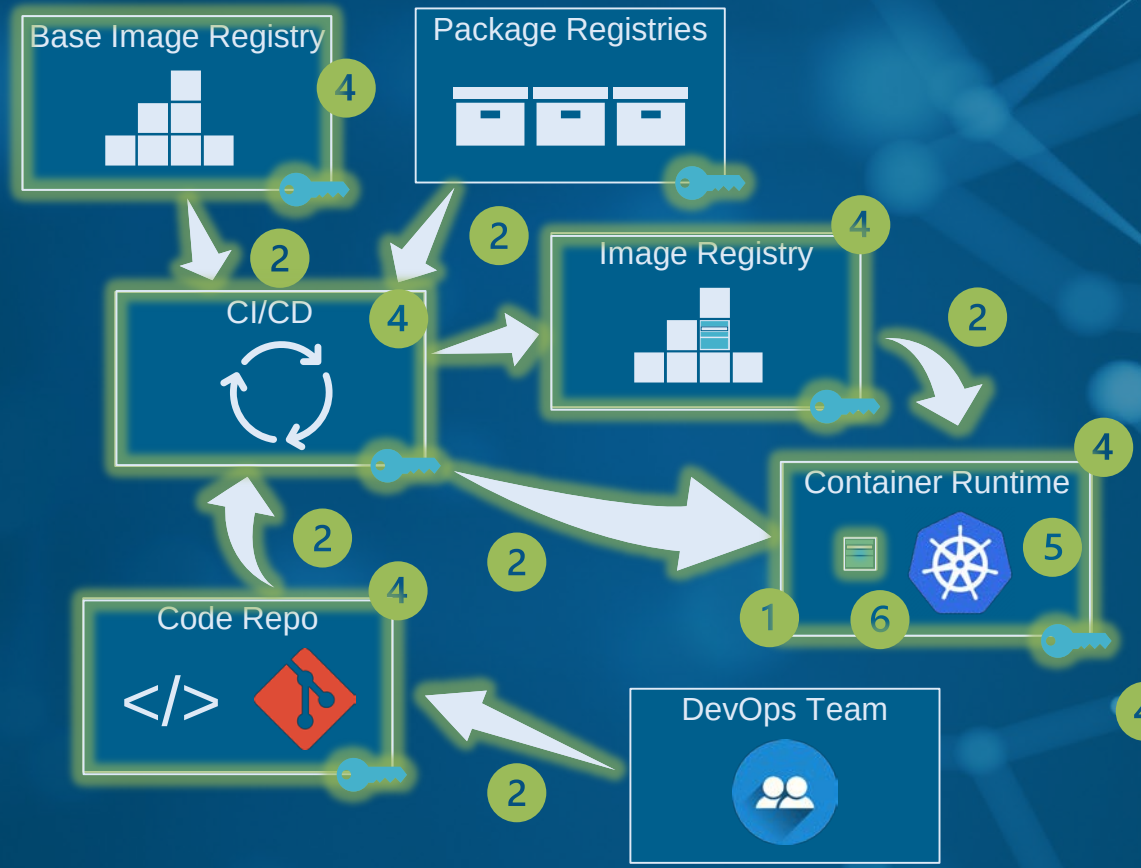
controlware



1. Trusted/internal Registries
2. Verified Images (hash/sign)
3. Infrastructure-as-Code (IaC)
4. Image Vulnerability Scanning
5. Container Vulnerability Scanning
6. Perimeter Security (inkl. egress)

Mehr gute Geister

controlware



1. Used Image Scanning
2. Schütze die Supply Chain
3. IAM, Auth, AuthZ, Least Privilege
4. Audit Logs
5. Intra-Cluster Firewalling
6. Behavior Analysis

Mehr gute Geister

controlware

Base Image Registry

Package Registries

Image Registry

CI/CD

Container Runtime

Code Repo

DevOps Team

IAM / Auth

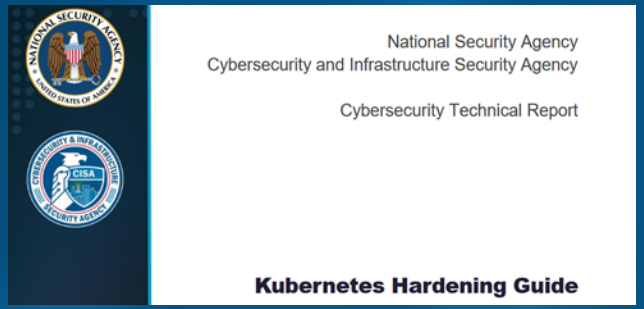
Die NSA sagt:

Die drei Hauptgründe für einen kompromittierten Kubernetes Cluster sind Supply Chain Angriffe, böswillige Akteure und Bedrohungen von innen.[1]

- Image Scanning
- Schütze die Supply Chain
- IAM, Auth, AuthZ, Least Privilege
- Audit Logs
- Intra-Cluster Firewalling
- Behavior Analysis

[1] https://www.bleepingcomputer.com/news/security/nsa-and-cisa-share-kubernetes-security-recommendations/

Unverändert wichtig: Hardening



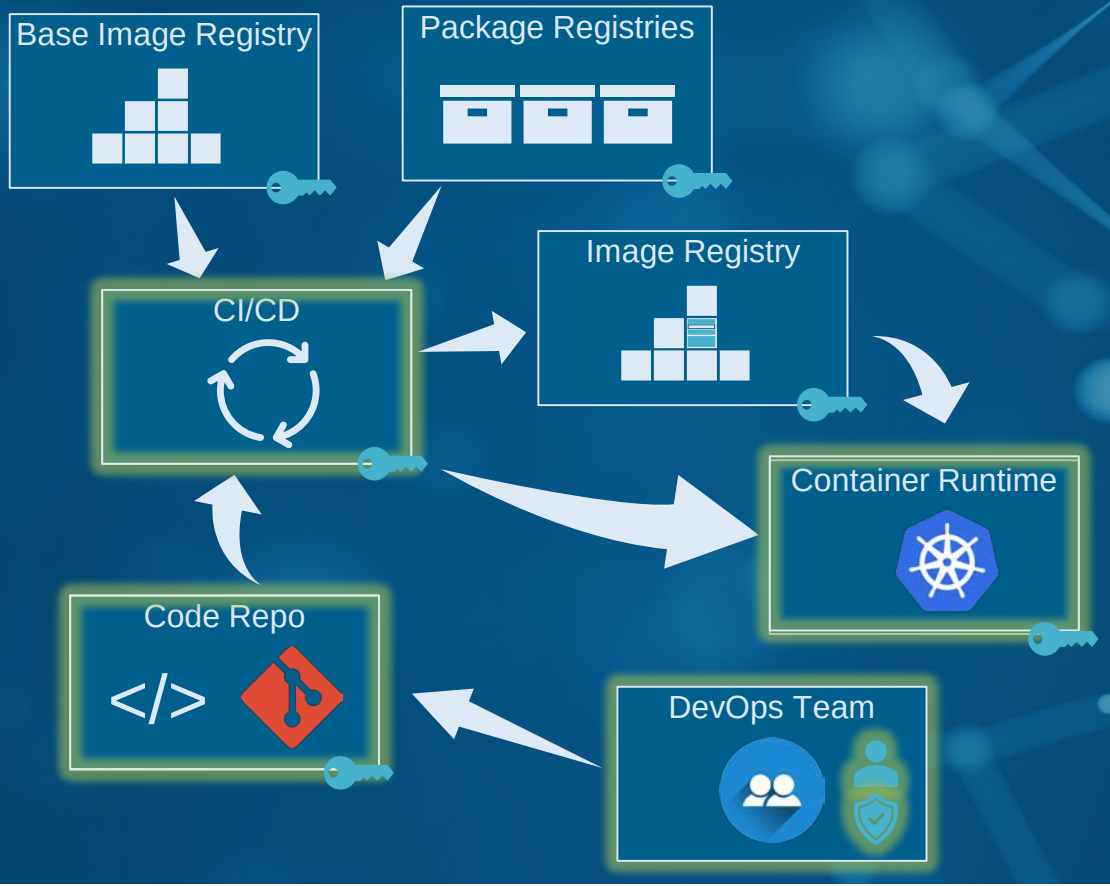
- "Non-root" containers
- Immutable container filesystems
- Pod Security Standards
- Network Policies
- External Secrets Providers
- Node Image Patching

https://media.defense.gov/2021/Aug/03/2002820425/-1/-1/1/CTR_KUBERNETES%20HARDENING%20GUIDANCE.PDF

Conclusio

Conclusio

controlware



DevOps und agile Entwicklung sind Teil des Problems und Teil der Lösung.

Policy as Code

Security Champions

Conclusio

controlware

DevOps und agile Entwicklung sind Teil des Problems und Teil der Lösung.

Etablierte Security Prinzipien und Tools sind auch im Container-Umfeld weiterhin hochrelevant.

Container Angriffe sind mitunter schwer zu erkennen. Setze an der Quelle an!

Automatisierung!

Automatisierung!

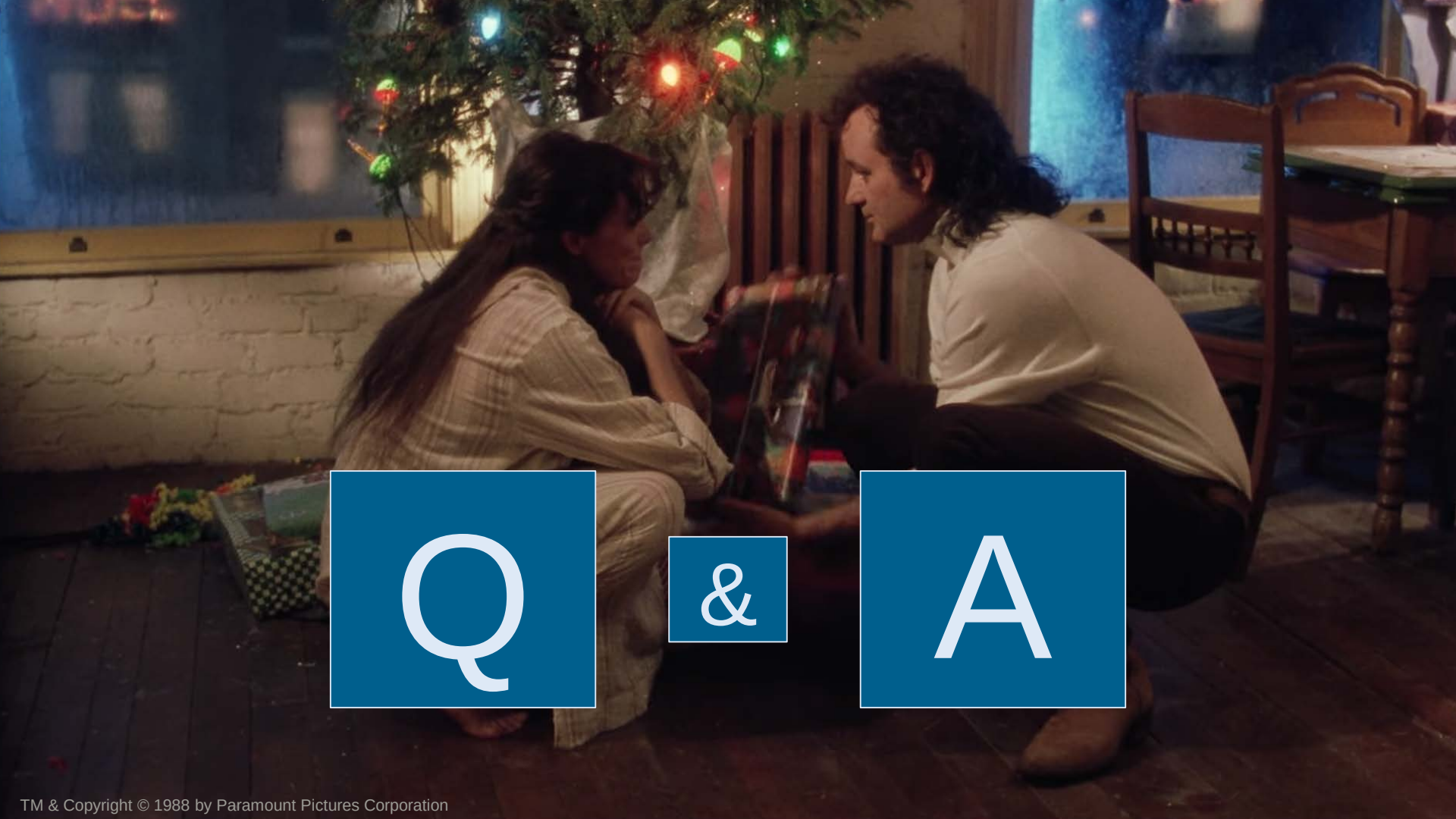
Automatisierung!

controlware

Vielen Dank für Ihre Aufmerksamkeit!
Thanks a bunch for your attention!

... und Frohe Weihnachten!

www.controlware.de



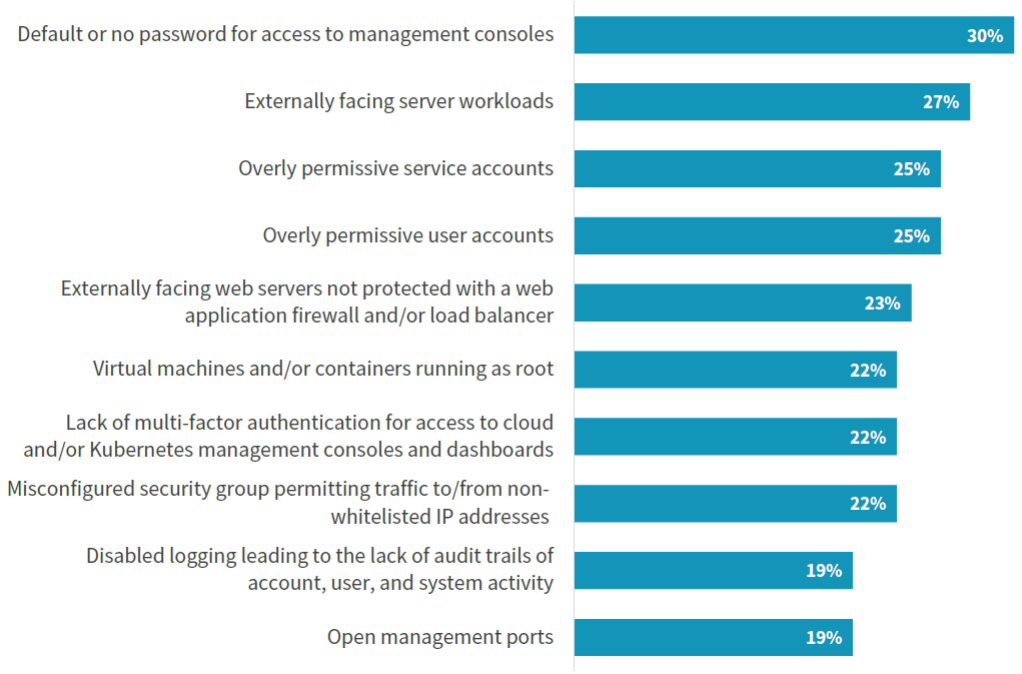
controlware

Backup

Alte und neue Bedrohungen

controlware

Ten most common cloud misconfigurations in the past 12 months.



Quelle: The Enterprise Strategy Group, The Maturation of Cloud-native Security, März 2021

Threat Matrix for Kubernetes

controlware

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Images from a private registry	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account		Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Quelle: Microsoft (https://www.microsoft.com/security/blog/2021/07/21/the-evolution-of-a-matrix-how-attck-for-containers-was-built/)