

7 июня 2023 📍 Москва, МЦК ЗИЛ

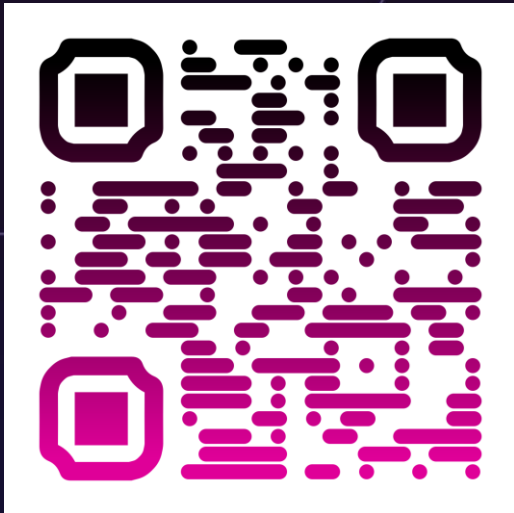
БЕКОН²³

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред

K8s в PCI DSS

Маркелов Александр

- Эксперт Райффайзен Банка
- Занимаюсь безопасностью облачной инфраструктуры более 2-х лет
- Курировал процесс аудита PCI DSS для K8s



Что такое PCI DSS?

БЕКОН

Стандарт PCI DSS — это международный стандарт безопасности, созданный специально для защиты данных платежных карт. Он позволяет защитить организацию от инцидентов безопасности и обеспечить необходимый уровень защищенности во всей платежной системе.



С точки зрения Kubernetes

БЕКОН

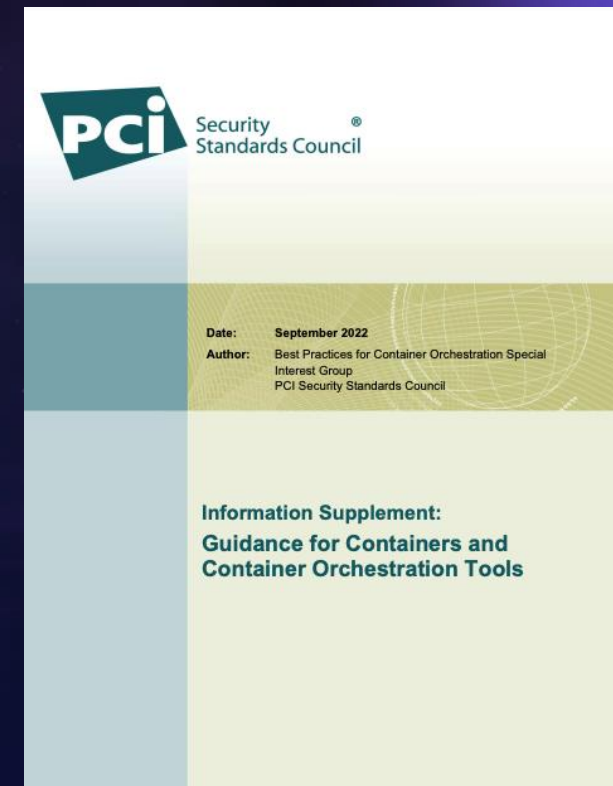
- НСПК требует соответствия PCI DSS
- Существует руководство по безопасности для контейнеров и оркестраторов контейнеров

Стандарт PCI DSS

В ПС «Мир» для обеспечения безопасности данных карт «Мир» используется международный индустриальный стандарт PCI Data Security Standard (PCI DSS)

Этот стандарт должен применяться всеми организациями, которые хранят, обрабатывают и передают данные карт «Мир». К таким организациям относятся и торгово-сервисные предприятия, которые принимают к оплате карты «Мир».

Стандарт PCI DSS — это международный стандарт безопасности, созданный специально для защиты данных платежных карт. Он позволяет защитить организацию от инцидентов безопасности и обеспечить необходимый уровень защищенности во всей платежной системе.



Дата выхода: сен 2022

Включает в себя:

- 16 модулей
- 42 рекомендации

- Authentication
- Authorization
- Workload Security
- Network Security
- PKI
- Secrets Management
- Container Orchestration Tool Auditing
- Container Monitoring
- Container Runtime Security
- Patching
- Resource Management
- Container Image Building
- Registry
- Version Management
- Configuration Management
- Segmentation

- **Authentication**
- **Authorization**
- ~~Workload Security~~
- **Network Security**
- ~~PKI~~
- ~~Secrets Management~~
- ~~Container Orchestration Tool Auditing~~
- **Container Monitoring**

- **Container Runtime Security**
- ~~Patching~~
- ~~Resource Management~~
- ~~Container Image Building~~
- ~~Registry~~
- ~~Version Management~~
- **Configuration Management**
- **Segmentation**


Authentication/Authorization

Проверяем:

- API
- Kubelet API
- Controller Manager
- Scheduler
- Etcd
- Межсервисное взаимодействие

Инструменты:

- CIS + kube-bench

	
1.2 API Server.....58	
1.2.1 Ensure that the --anonymous-auth argument is set to false (Manual)	59
1.2.2 Ensure that the --token-auth-file parameter is not set (Automated)	61
1.2.3 Ensure that the --DenyServiceExternalIPs is not set (Automated).....	63
1.2.4 Ensure that the --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate (Automated).....	65
1.2.5 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Automated)	67
1.2.6 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Automated)	69
1.2.7 Ensure that the --authorization-mode argument includes Node (Automated).....	71
1.2.8 Ensure that the --authorization-mode argument includes RBAC (Automated).....	73
1.2.9 Ensure that the admission control plugin EventRateLimit is set (Manual)	75
1.2.10 Ensure that the admission control plugin AlwaysAdmit is not set (Automated).....	77
1.2.11 Ensure that the admission control plugin AlwaysPullImages is set (Manual).....	79
1.2.12 Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not	
CIS Benchmark Recommendation	
4.1.4	If proxy kubeconfig file exists ensure ownership root:root (Manual)
4.1.5	Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive (Automated)
4.1.6	Ensure that the --kubeconfig kubelet.conf file ov is set to root:root (Automated)
4.1.7	Ensure that the certificate authorities file permis set to 600 or more restrictive (Manual)
4.1.8	Ensure that the client certificate authorities file c is set to root:root (Manual)

Тезисы:

- **cluster-admin ЗЛО!**
- Аутентификация по токенам - боль
- Не можешь отозвать – не используй
- SA нужны не всем и не всегда
- За SA default нужно следить
- MFA наше все

Решения:

- policy engine (Для SA)
- IM/PAM (для пользователей)

Полезные ссылки:

[Ссылка на политику контроля привилегий SA](#)



Network Security

Тезисы:

- Сетевые политики нужны
- Сделаем удобно
- Запретим все по умолчанию
- А как контролировать?

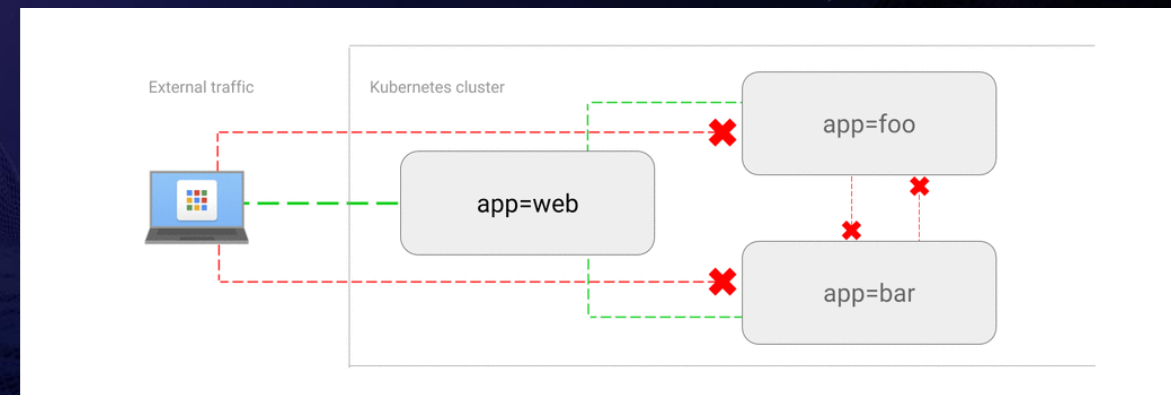
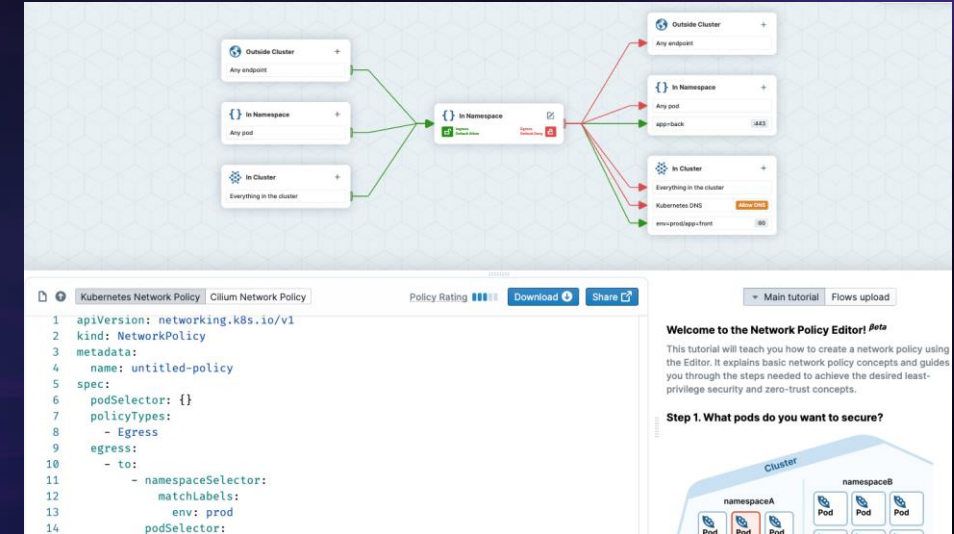
Решения:

- CNI поддерживающий NP
- CSP как класс решений
- Autogen NP
- policy engine

Полезные ссылки:

[Политика для kubernetes которая создает default-deny NP](#)

[Запретить ingress трафик](#)



Runtime Security

Тезисы:

- Логи во внешнюю систему
- Отслеживаем изменения
- Сторонние решения поведенческого анализа

Решения:

- Falco
- CSP как класс решений



Suspicious Filesystem Changes

High Severity Event ID: 173456b09fbf27b3945cdefcaf32f3bf

View Activity Audit

Policy & Triggered Rules

Edit Policy

name Suspicious Filesystem Changes

ruleType Falco - Syscall

ruleName Modify Shell Configuration File

a shell configuration file has been modified (user.name=root user.loginuid=-1 proc.cmdline=mkhomedir proc.pcmdline=odddjobd -n -p /run/odddjobd.pid -t 300 file=/home/admmdeq/.zshrc container.id=host evt.type=openat evt.res=SUCCESS proc.pid=2395381 proc.cwd=/ proc.ppid=1304 proc.sid=1304 proc.exepath=/usr/libexec/odddjob/mkhomedir user.uid=0 user.loginname=<NA> group.gid=0 group.name=root container.name=host image=<NA>)

file	directory /var/lib/rpm/	filename .dbenv.lock	comm dnf	permissions rw					
file	directory /var/cache/dnf/	filename tempfiles.json	comm dnf	permissions w					
file	directory /var/cache/dnf/	filename expired_repos.json	comm dnf	permissions w					
file	directory /run/rhsm/	filename cert.pid	comm dnf	permissions rw					
file	directory /run/rhsm/	filename cert.pid	comm dnf	permissions w					
file	directory /run/rhsm/	filename cert.pid	comm dnf	permissions rw					
file	directory /var/lib/rhsm/cache/	filename profile.json	comm dnf	permissions rw					
net	process name dnf	direction out	l4protocol tcp	client ipv4: 10.242.234.4	client port 39748	server ipv4 10.243.33.138	server port 8443	pid 2395484	
net	process name dnf	direction out	l4protocol tcp	client ipv4: 10.242.234.4	client port 39734	server ipv4 10.243.33.138	server port 8443	pid 2395484	
net	process name dnf	direction out	l4protocol tcp	client ipv4: 10.242.234.4	client port 45446	server ipv4 10.243.33.138	server port 443	pid 2395484	

Configuration Management


```
74 PLAY [CIS] *****
75 TASK [../roles/cis : 1.1.1 | MASTER | Set API server pod specification file permissions to 600] ***
76 ok: [s-msk-t-acq-km3]
77 ok: [s-msk-t-acq-km2]
78 ok: [s-msk-t-acq-km1]
79 TASK [../roles/cis : 1.1.2 | MASTER | Set API server pod specification file ownership to root:root] ***
80 ok: [s-msk-t-acq-km2]
81 ok: [s-msk-t-acq-km1]
82 ok: [s-msk-t-acq-km3]
83 TASK [../roles/cis : 1.1.3 | MASTER | Ensure that the controller manager pod specification file permissions are set to 600] ***
84 ok: [s-msk-t-acq-km1]
85 ok: [s-msk-t-acq-km2]
86 ok: [s-msk-t-acq-km3]
87 TASK [../roles/cis : 1.1.4 | MASTER | Ensure that the controller manager pod specification file ownership is set to root:root] ***
88 ok: [s-msk-t-acq-km1]
89 ok: [s-msk-t-acq-km2]
90 ok: [s-msk-t-acq-km3]
91 TASK [../roles/cis : 1.1.5 | MASTER | Ensure that the scheduler pod specification file permissions are set to 600] ***
92 ok: [s-msk-t-acq-km1]
93 ok: [s-msk-t-acq-km3]
94 ok: [s-msk-t-acq-km2]
95 TASK [../roles/cis : 1.1.6 | MASTER | Ensure that the scheduler pod specification file ownership is set to root:root] ***
96 ok: [s-msk-t-acq-km1]
97 ok: [s-msk-t-acq-km3]
98 ok: [s-msk-t-acq-km2]
99 TASK [../roles/cis : 1.1.7 | MASTER | Ensure that the etcd pod specification file permissions are set to 600] ***
100 changed: [s-msk-t-acq-km3]
101 changed: [s-msk-t-acq-km1]
102 changed: [s-msk-t-acq-km2]
103 TASK [../roles/cis : 1.1.8 | MASTER | Ensure that the etcd configuration file ownership is set to root:root] ***
104 changed: [s-msk-t-acq-km1]
105 changed: [s-msk-t-acq-km2]
106 changed: [s-msk-t-acq-km3]
107 TASK [../roles/cis : 1.1.9 | Find Container Network Interface files] *****
108 ok: [s-msk-t-acq-km3]
109 ok: [s-msk-t-acq-km1]
110 ok: [s-msk-t-acq-km2]
```

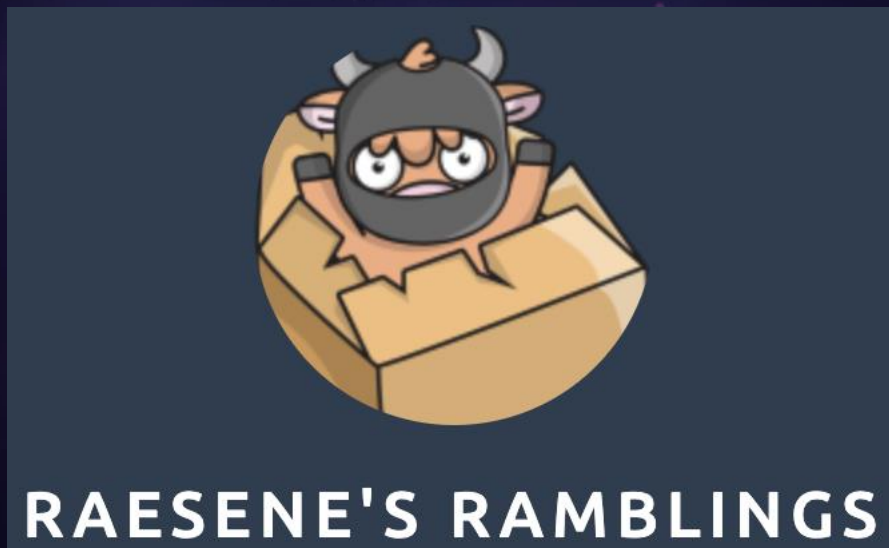
PipelineNeedsJobs23Failed Jobs1Tests113

< kube-bench

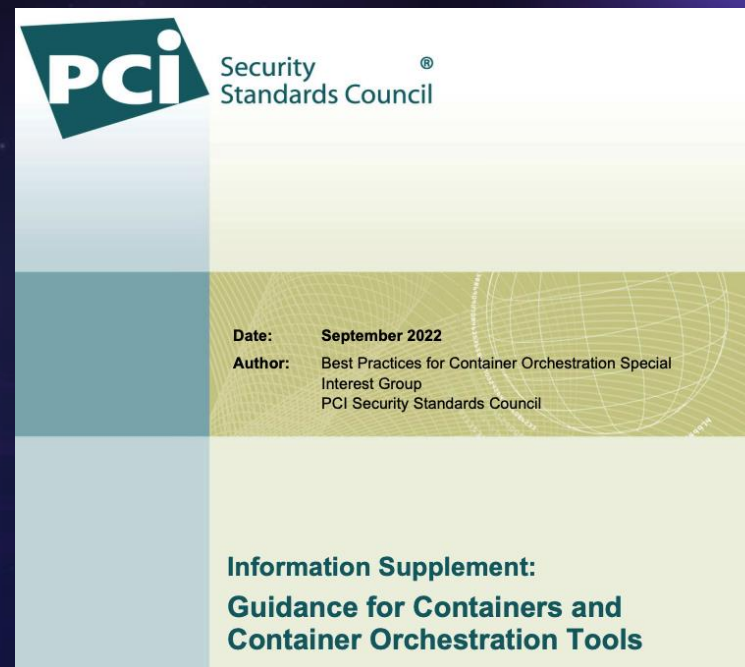
113 tests1 failures0 errors98.72% success rate0.00ms

Tests

Suite	Name	Filename	Status	Duration	Details
Master Node Configuration Files	1.1.19 Ensure that the Kubernetes PKI directory and file ownership is set to root:root (Automated)		<div>✖</div>	0.00ms	<div>View details</div>
Master Node Configuration Files	1.1.1 Ensure that the API server pod specification file permissions are set to 644 or more restrictive (Automated)		<div>✔</div>	0.00ms	<div>View details</div>
Master Node Configuration Files	1.1.2 Ensure that the API server pod specification file ownership is set to root:root (Automated)		<div>✔</div>	0.00ms	<div>View details</div>
Master Node Configuration Files	1.1.3 Ensure that the controller manager pod specification file permissions are set to 644 or more restrictive (Automated)		<div>✔</div>	0.00ms	<div>View details</div>

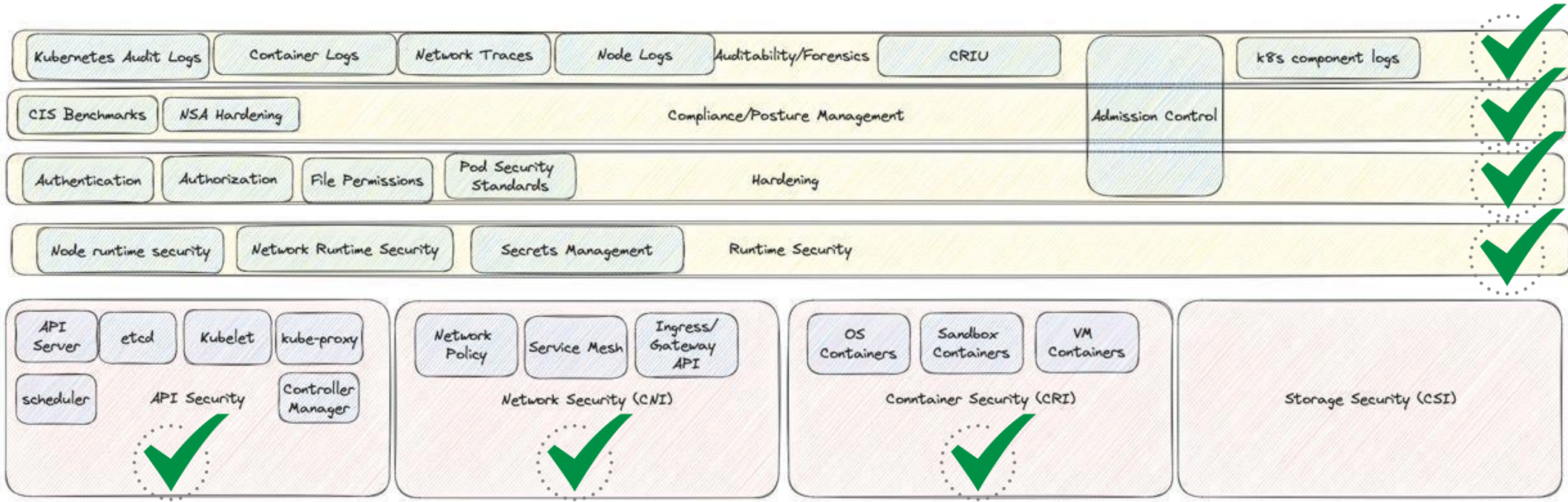


Подробный разбор требований с общими рекомендациями



Перечень требований и рекомендаций

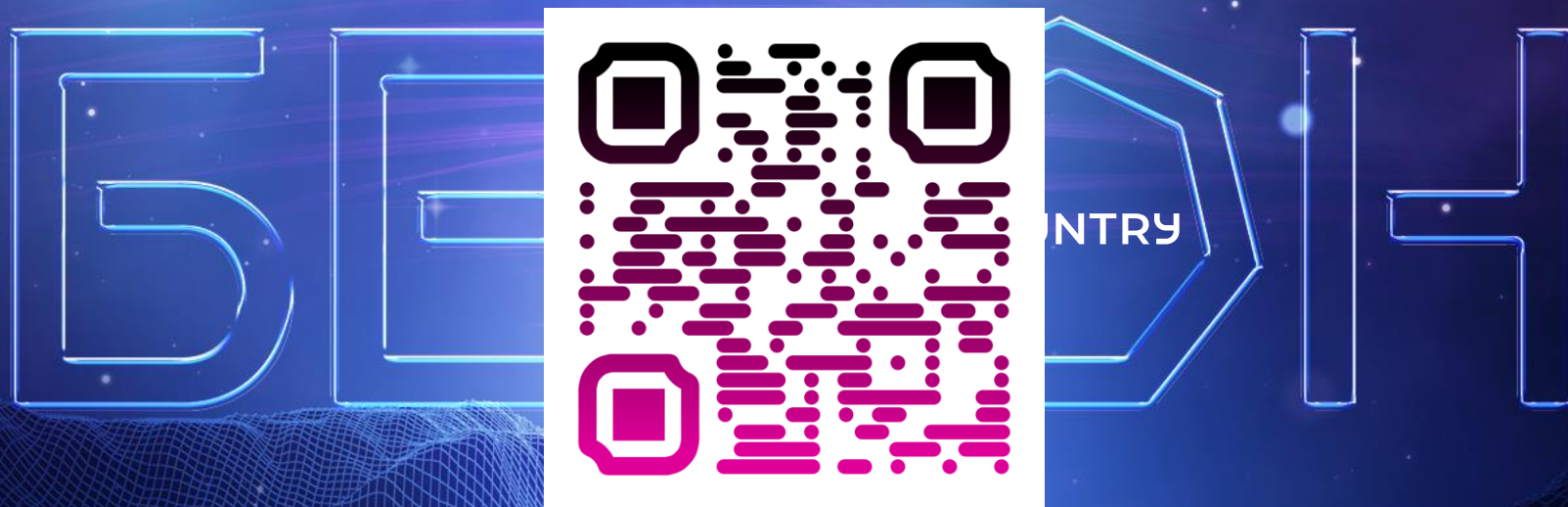
NB the scope of this is purely Kubernetes and necessary infrastructure, so not considering Cloud security or the security of application code running in the cluster



Источник

7 июня 2023 📍 Москва, МЦК ЗИЛ

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред



Контакты:

Tg: @AVmarke