СБЕР ЗДОРОВЬЕ

# Применение kyverno в крупной компании

СБЕР ЗДОРОВЬЕ

# Александр Телевной

Head of DevOps
СберЗдоровье

Systems Engineer с 2016

СБЕР ЗДОРОВЬЕ

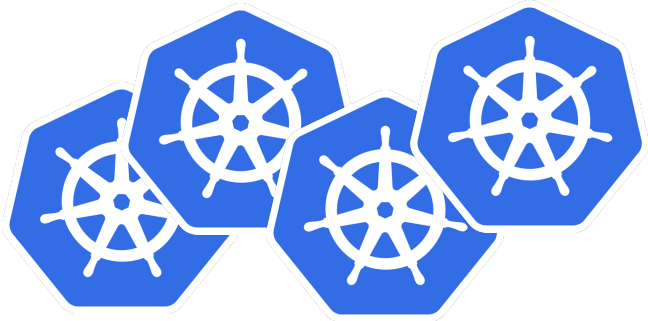
# Why? What? DoD?

# Why:

СБЕР ЗДОРОВЬЕ

**01** **Инфраструктура:**

У нас есть 10 K8S кластеров и 20 команд которые работаю в разных стеках и в разных департаментах



**02** **Срочная задача:**

К нам пришли сотрудники CS и просят срочно внедрить меры по запрету небезопасных конфигурации в K8S


**03** **Список политик:**

Запрет на privileged mode и Host network

# What:

СБЕР ЗДОРОВЬЕ

**01** **Внедрить политики:**

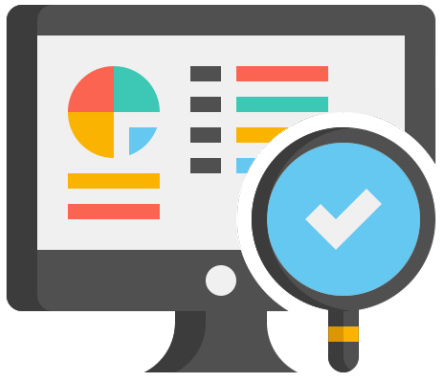
Которые будут запрещать запуск ресурсов в K8S в незащищенной конфигурации

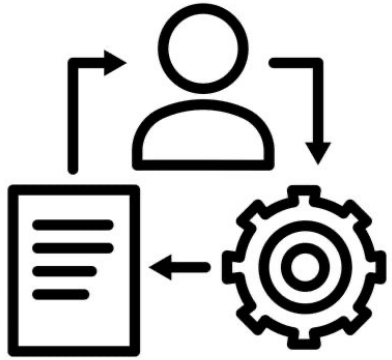
**02** **Мониторинг:**

Мы должны понимать что соответствует политикам, а что нет

**03** **Процесс внедрения политик:**

После применения базовых политик, появится желание добавить что-то еще





# DoD:

СБЕР ЗДОРОВЬЕ

**01** **Внедрить политики: 100%**

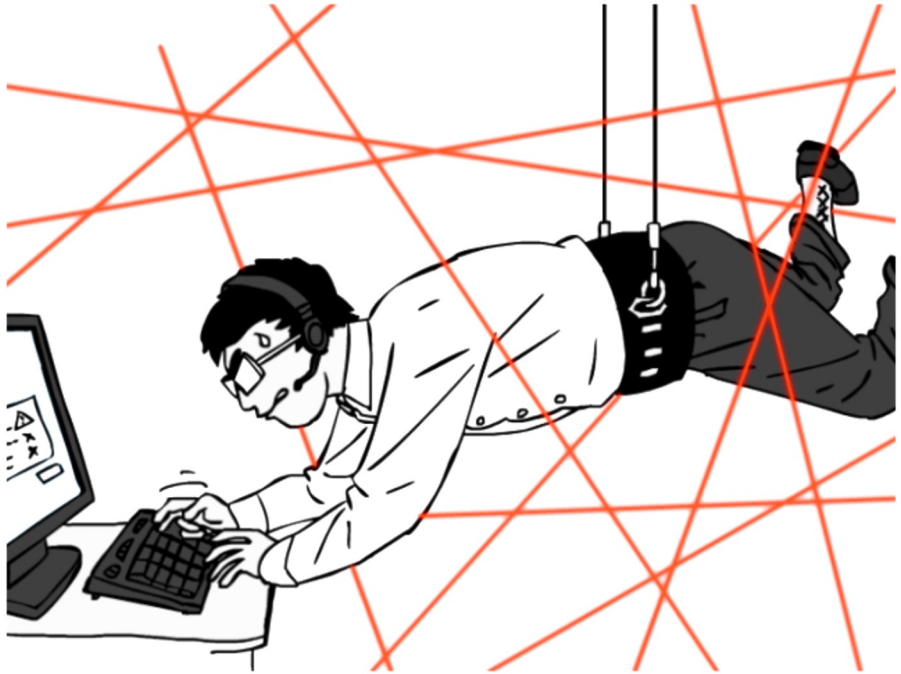
Которые будут запрещать запуск ресурсов в K8S в незащищенной конфигурации

**02** **Мониторинг: 100%**

Мы должны понимать что соответствует политикам, а что нет

**03** **Процесс внедрения политик: создан**

После применения базовых политик, появится желание добавить что-то еще

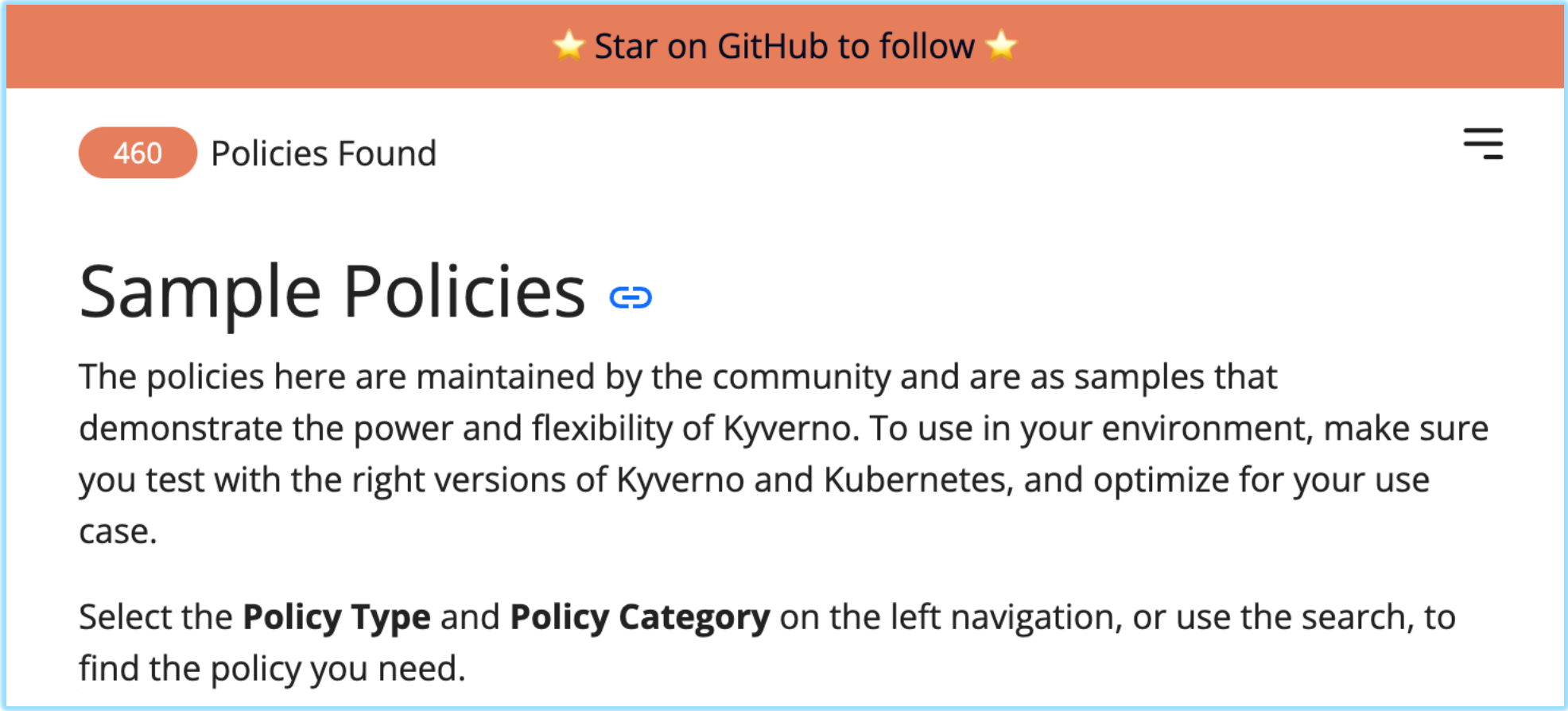


СБЕР ЗДОРОВЬЕ

# Этот доклад не про написание политик

# https://kyverno.io/policies/

СБЕР ЗДОРОВЬЕ

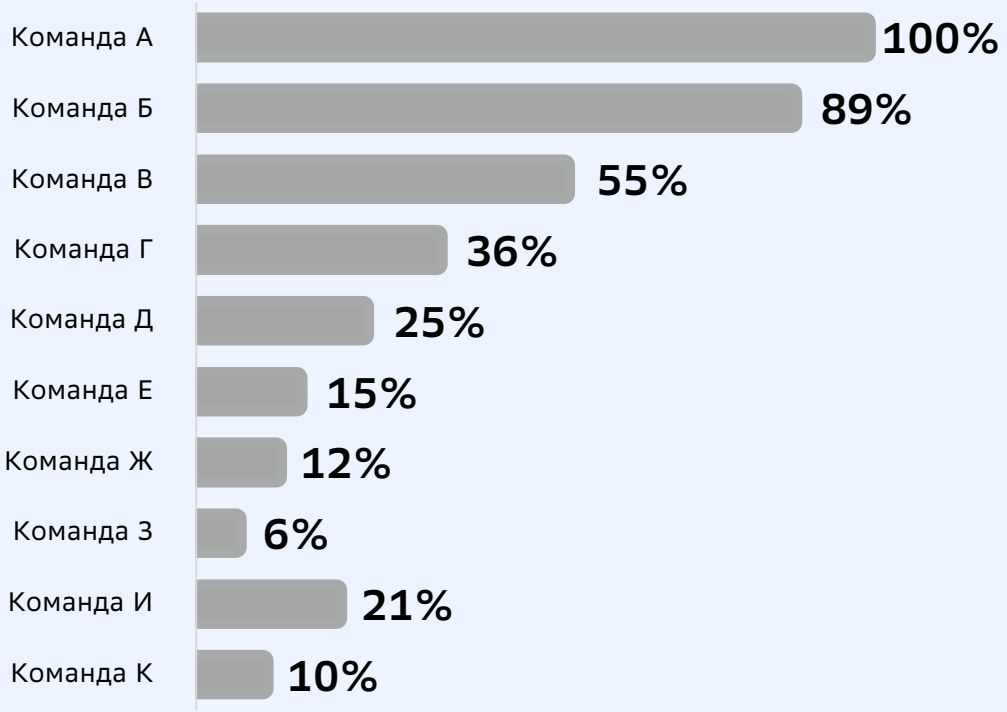


# Вопрос №1

Скорость внедрения изменений и их приоритеты

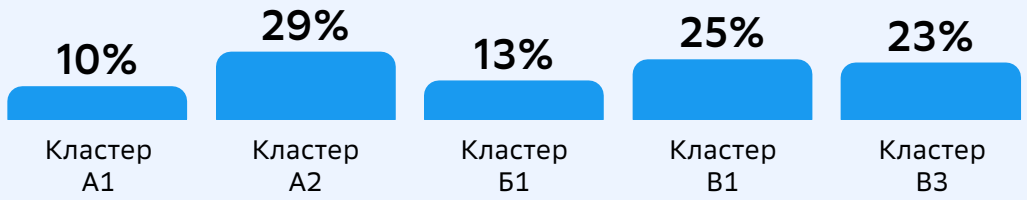
СБЕР ЗДОРОВЬЕ

## Распределение по командам:




## Распределение по департаментам:


## Распределение по кластерам:



# Вопрос №1

Скорость внедрения изменений и их приоритеты

СБЕР ЗДОРОВЬЕ

**01** **Внедряем политику уже на 80%**

Остальные 20% добавляем в исключения и создаем фокусные задачи

**02** **Внедряем исключение на уровне не доступном командам**

Мы создаем ns через terraform и изменения в ns руками будут быстро замечены

**03** **Каждая политика может быть добавлена в исключения независимо**

Мы можем гранулярно включать политики по мере готовности команд

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: sa-restricted
spec:
  rules:
    - name: sa-restricted
      match:
        all:
        - resources:
            kinds:
            - Pod
      exclude:
        any:
        - resources:
            namespaceSelector:
              matchLabels:
                skip-policies.kyverno.io/sa-restricted: "true"
        - resources:
            namespaces:
            - "kube-*"
            - "kyverno"
      validate:
        failureAction: Enforce
        message: "automountServiceAccountToken must be false"
        pattern:
          spec:
            automountServiceAccountToken: "false"
```

# Вопрос №2

Тестирование политик

СБЕР ЗДОРОВЬЕ

```yaml
apiVersion: cli.kyverno.io/v1alpha1
kind: Test
metadata:
  name: servicelinks-false
policies:
- ../servicelinks-false.yaml
resources:
- pod.yaml
variables: var.yaml
results:

- policy: servicelinks-false
  rule: servicelinks-false
  kind: Pod
  resources:
  - good-pod-with-skip
  - bad-pod-with-skip
  result: skip

- policy: servicelinks-false
  rule: servicelinks-false
  kind: Pod
  resources:
  - good-pod-without-skip
  result: pass

- policy: servicelinks-false
  rule: servicelinks-false
  kind: Pod
  resources:
  - bad-pod-without-skip
  result: fail
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: bad-pod-with-skip
  namespace: ns-with-skip
spec:
  containers:
    - name: alpine
      image: alpine
      command: ["sleep","10000"]
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: good-pod-without-skip
spec:
  enableServiceLinks: "false"
  containers:
    - name: ubuntu
      image: ubuntu
      command: ["sleep","10000"]
```

```yaml
apiVersion: cli.kyverno.io/v1alpha1
kind: Values
metadata:
  name: servicelinks-false
namespaceSelector:
  - name: ns-with-skip
    labels:
      skip-policies.kyverno.io/servicelinks-false: "true"
```

```
❯ kyverno test ./servicelinks-false --remove-color
Loading test  ( servicelinks-false/kyverno-test.yaml ) ...
  Loading values/variables ...
  Loading policies ...
  Loading resources ...
  Loading exceptions ...
  Applying 1 policy to 4 resources with 0 exceptions ...
  Checking results ...

┌────┬──────────────────┬──────────────────┬──────────────────────────────────────┬────────┬─────────┐
│ ID │ POLICY           │ RULE             │ RESOURCE                             │ RESULT │ REASON  │
├────┼──────────────────┼──────────────────┼──────────────────────────────────────┼────────┼─────────┤
│ 1  │ servicelinks-false │ servicelinks-false │ v1/Pod/Pod                         │ Pass   │ Excluded │
│ 2  │ servicelinks-false │ servicelinks-false │ v1/Pod/Pod                         │ Pass   │ Excluded │
│ 3  │ servicelinks-false │ servicelinks-false │ v1/Pod/default/good-pod-without-skip │ Pass   │ Ok      │
│ 4  │ servicelinks-false │ servicelinks-false │ v1/Pod/default/bad-pod-without-skip  │ Pass   │ Ok      │
└────┴──────────────────┴──────────────────┴──────────────────────────────────────┴────────┴─────────┘


Test Summary: 4 tests passed and 0 tests failed
```

# Вопрос №3

Kyverno не только для CS, но и для IT

СБЕР ЗДОРОВЬЕ

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: nginx-depricated
spec:
  rules:
    - name: nginx-depricated
      match: …
      exclude: …
      preconditions:
        all:
        - key: "{{ request.object.spec.[initContainers, containers][].image }}"
          operator: AnyIn
          value: "nginx:*"
      validate:
        failureAction: Enforce
        message: "nginx must have tag > 1.25"
        foreach:
        - list: "request.object.spec.containers"
          anyPattern:
          - image: nginx:1.26*
          - image: nginx:1.27*
          - image: nginx:1.28*
          - image: nginx:1.29*
          - image: nginx:1.3*
          - image: nginx:2*
```

# PS

СБЕР ЗДОРОВЬЕ

**01** **Всегда используйте kyverno в HA режиме в PROD**

Иначе не сможете поднять kyverno без kyverno

**02** **Не используйте mutate политики**

Если придется отключить kyverno, то вы не просто отключить фильтры, вы не сможете запустить правильно то что модифицируется

**03** **Тесты можно передать в команды для проверки манифестов в CI/CD**

Новые сервисы со 100% гарантией в PROD деплоятся с первого раза

СБЕР ЗДОРОВЬЕ

# Спасибо за внимание