

7 июня 2023 📍 Москва, МЦК ЗИЛ

БЕКОН²³

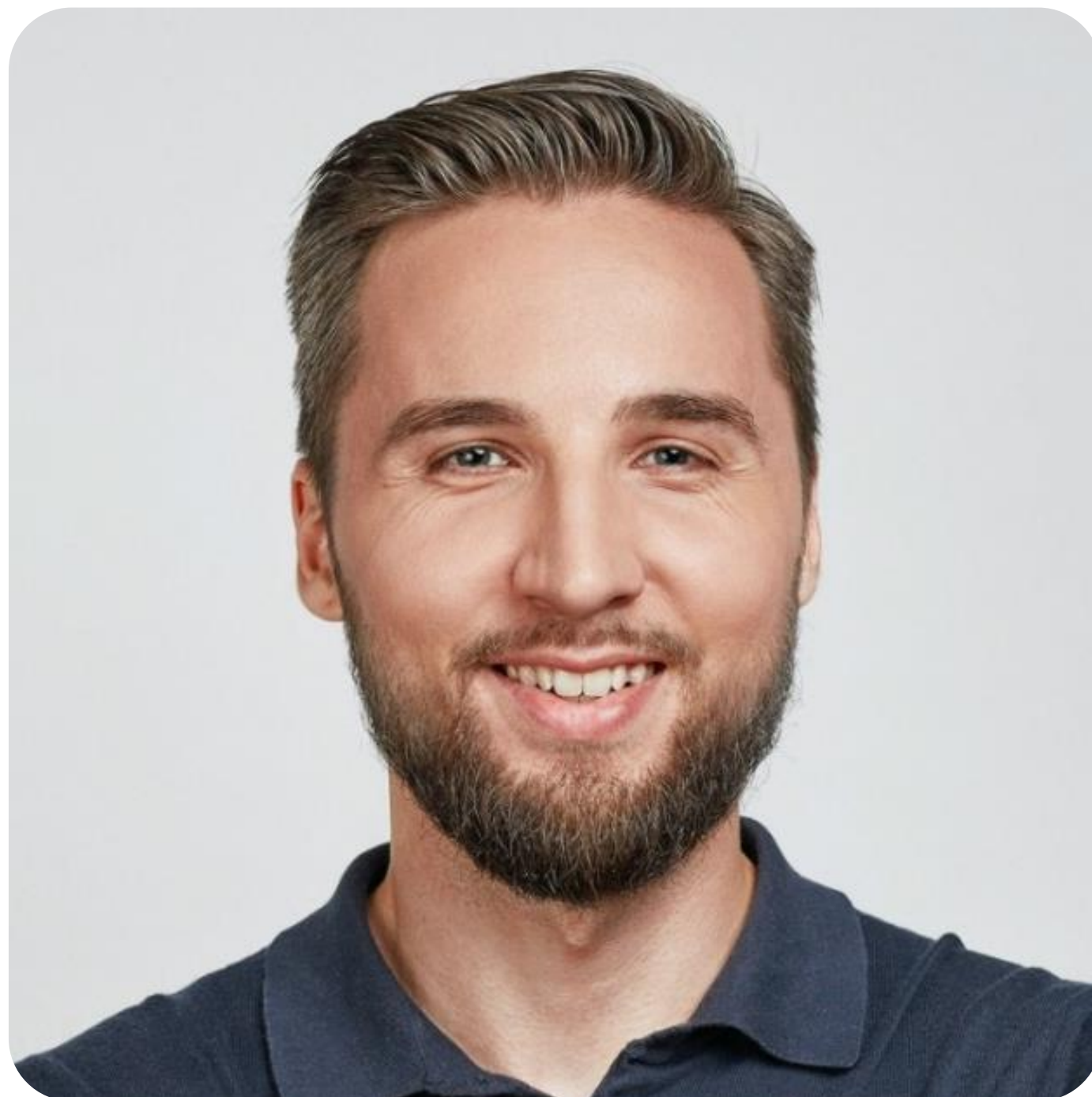
Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред

Как правильно готовить Kuberно и работать с его алертами

Миртов Алексей

Руководитель группы продуктовой архитектуры Security & Compliance

Yandex.Cloud



2023



Руководитель продуктовой
архитектуры Security

Yandex.Cloud

Эксперт в безопасности

Сетях и контейнерах: СКА, Palo Alto Networks (PSE), Check Point
CSA, BSI ISO 27001:2013, PentestIT

Выстроил цикл безопасной разработки

В команде 400+ разработчиков
для ИТ-системы на базе Kubernetes® в облаке

Проектировал и реализовал Security
Operational Center в Казахстане

10+ лет опыт работы в ИБ

1. Нюансы настройки Kuberно
2. Audit logs. На что реагировать
3. А в какую сторону двигаться дальше?

Kyverno

Kyverno



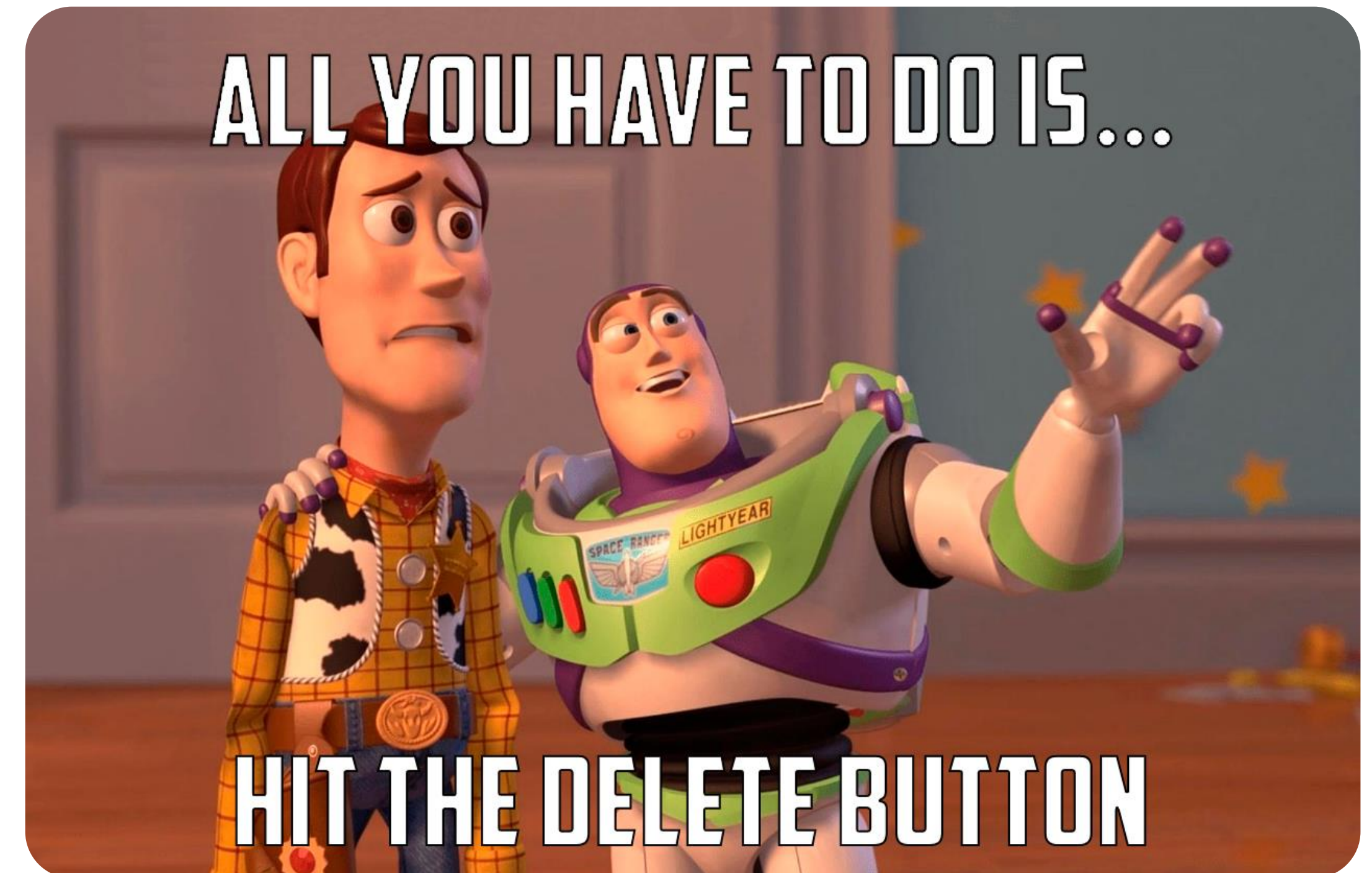
- Admission controller
- K8s like язык политик
- Большая поддержка community (набор готовых политик)
- Удобная отправка репортов
- Многие считают, что более удачный, чем аналоги (включая нативные K8s)

Надёжность #1

Что будет, если удалить Kyverno из кластера?

- Удаление Deployment — игнорируются политики
- Удаление Validating admission webhook — игнорируются политики

Не забудьте среагировать на удаление в SIEM



Надёжность #2

Что будет, если Kverno недоступен?

- failurePolicy: "Fail" — не пропускает
- failurePolicy: "Ignore" — пропускает

Для критичных политик можно выставлять на уровне Policy

Policy Settings

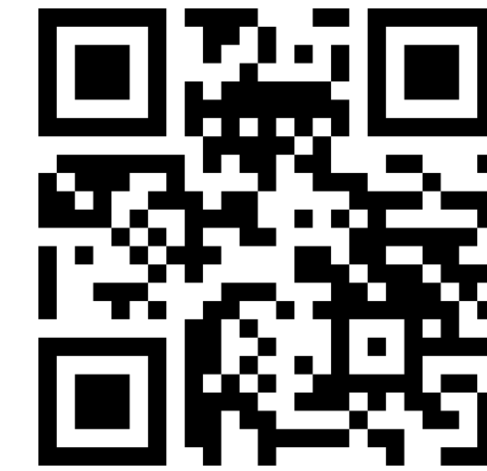
Common configuration for all rules in a policy.

A [policy](#) contains one or more rules, and the following common settings which apply to all rules in the policy:

- **applyRules:** States how many of the rules in the parent policy should be applied to a matching resource. Values are [One](#) and [All](#) (default). If set to [One](#), the first matching rule to be applied will stop further rules from being evaluated.
- **validationFailureAction:** controls if a validation policy rule failure should block the admission review request ([Enforce](#)) or allow ([Audit](#)) the admission review request and report the policy failure in a policy report. Defaults to [Audit](#).
- **validationFailureActionOverrides:** a ClusterPolicy attribute that specifies [validationFailureAction](#) Namespace-wise. It overrides [validationFailureAction](#) for the specified Namespaces.
- **background:** controls if rules are applied to existing resources during a background scan. Defaults to "true".
- **schemaValidation:** controls whether policy validation checks are applied. Defaults to "true". Kverno will attempt to validate the schema of a policy and fail if it cannot determine it satisfies the OpenAPI schema definition for that resource. Can occur on either validate or mutate policies. Set to "false" to skip schema validation.
- **failurePolicy:** defines the API server behavior if the webhook fails to respond. Allowed values are "Ignore" or "Fail". Defaults to "Fail". Additionally, in 1.8.0, if set to "Ignore" will allow failing calls to image registries to be ignored. This allows for rule types like `verifyImages` or others which use image data to not block if the registry is temporarily down, useful in situations where images already exist on the nodes.
- **webhookTimeoutSeconds:** specifies the maximum time in seconds allowed to apply this policy. The default timeout is 10s. The value must be between 1 and 30 seconds.

- **failurePolicy:** defines the API server behavior if the webhook fails to respond. Allowed values are "Ignore" or "Fail". Defaults to "Fail". Additionally, in 1.8.0, if set to "Ignore" will allow failing calls to image registries to be ignored. This allows for rule types like `verifyImages` or others which use image data to not block if the registry is temporarily down, useful in situations where images already exist on the nodes.

Надёжность #3



clck.ru/34S2fw

Рекомендации High Availability

`replicaCount: 3` (по дефолту не установлен)

`podDisruptionBudget:`

-- Configures the minimum available pods
for kyverno disruptions.

Cannot be used if `maxUnavailable` is set.

`minAvailable: 1`

-- Configures the maximum unavailable pods
for kyverno disruptions.

Cannot be used if `minAvailable` is set.

`maxUnavailable:`

`antiAffinity:`

-- Pod antiAffinities toggle.

Enabled by default but can be disabled

if you want to schedule pods to the same node.

`enable: true`

Kyverno policies

Kyverno policies

- Отдельный helm-chart
- Реализует Pod Security Standards
- Помогает управлять custom-политиками
- Управлять исключениями



Pod Security Standards

Это рекомендации K8s

- Baseline: с него можно начать
- Restricted: можно постепенно набирать критичные (начиная с detect)

Pod Security Standards

The Pod Security Standards define three different *policies* to broadly cover the security spectrum. These policies are *cumulative* and range from highly-permissive to highly-restrictive. This guide outlines the requirements of each policy.

Profile	Description
Privileged	Unrestricted policy, providing the widest possible level of permissions. This policy allows for known privilege escalations.
Baseline	Minimally restrictive policy which prevents known privilege escalations. Allows the default (minimally specified) Pod configuration.
Restricted	Heavily restricted policy, following current Pod hardening best practices.

Pod Security Standards

Это рекомендации K8s

- Baseline: с него можно начать
- Restricted: можно постепенно набирать критичные (начиная с detect)

Baseline

disallow-capabilities
disallow-host-namespaces
disallow-host-path
disallow-host-ports
disallow-host-process
disallow-privileged-containers
disallow-proc-mount
disallow-selinux
restrict-apparmor-profiles
restrict-seccomp
restrict-sysctls

Restricted

disallow-capabilities-strict
disallow-privilege-escalation
require-run-as-non-root-user
require-run-as-nonroot
restrict-seccomp-strict
restrict-volume-types

Пример

```
# -- Pod Security Standard profile (`baseline`, `restricted`, `privileged`, `custom`).  
# For more info https://kyverno.io/policies/pod-security.
```

```
podSecurityStandard: baseline
```

```
# -- Pod Security Standard (`low`, `medium`, `high`).
```

```
podSecuritySeverity: medium
```

```
# -- Policies to include when `podSecurityStandard` is `custom`.
```

```
podSecurityPolicies: []
```

```
# -- Additional policies to include from `other`.
```

```
includeOtherPolicies: []
```

```
# -- Additional policies to include from `restricted`.
```

```
includeRestrictedPolicies:
```

```
- require-run-as-nonroot
```

```
- restrict-seccomp-strict
```

```
failurePolicy: Fail
```


```
validationFailureAction: enforce
```

```
validationFailureActionByPolicy:
```

```
require-run-as-nonroot: audit
```

Best Practice политики из набора Kyverno

Add Network Policy	Для каждого нового ns добавляет сетевую политику default deny
Add Network Policy for DNS	Разрешает при этом доступ к dns
Block Ephemeral Containers	Блокирует kubectl debug и attach временных контейнеров
Block Pod Exec by Pod and Container	Блокирует exec в контейнеры



Policies

Pod Security

Gatekeeper Migration

Policy Type

- ☐ Generate
- ☐ Mutate
- ☐ Validate
- ☐ VerifyImages

Policy Category

- ☐ AWS
- ☐ Argo
- ☐ Best Practices
- ☐ Cert-Manager
- ☐ Consul
- ☐ EKS Best Practices
- ☐ ExternalSecretOperator

Custom-политики (самописные)



clck.ru/34S3G4

allow-actions-with-policys-only-silo-sa	Разрешает работу с ClusterPolicy только сервисному аккаунту управления ИБ
deny-attach-by-pod-and-container	Блокирует attach к контейнеру (позволяет выполнять команды)
mutate-securitycontext-seccomp	Принудительно добавляет в каждый deployment/pod RuntimeDefault профиль seccomp (защищает от множества уязвимостей)
restrict-image-registries	Разрешает загрузку образов только из «cr.yandex/*»

Нюансы с kubectl proxy и kubectl port-forward

Ссылка на issue



<https://clck.ru/34aLSy>

Нельзя написать политики

Ограничение API server, который отсылает только один из четырех actions в рамках webhook:

- CREATE
- UPDATE
- DELETE
- CONNECT

Proxy, port-forward — не относятся к ним

```
spec:
  validationFailureAction: enforce
  background: false
  rules:
  - name: deny-nginx-exec-in-myapp-maintenance
    match:
      any:
      - resources:
          kinds:
          - PodExecOptions
    preconditions:
      all:
      - key: "{{ request.operation || 'BACKGROUND' }}"
        operator: Equals
        value: CONNECT
      - key: "{{ request.name }}"
        operator: Equals
        value: myapp-maintenance*
    validate:
      message: Nginx containers inside myapp-maintenance Pods may not be exec'd into.
      deny:
        conditions:
          all:
          - key: "{{ request.object.container }}"
            operator: Equals
            value: nginx
```


Исключения #1

На уровне values чарта policies

Можно передавать эти values через Argo CD для разных кластеров через applications и labels после согласования PR в git

```
policyExclude: {}
# # Exclude resources from individual policies
# disallow-host-path:
# any:
# - resources:
#   kinds:
#   - Pod
#   namespaces:
#   - fluent
# # Policies with multiple rules can have individual rules excluded
# adding-capabilities-strict:
# any:
# - resources:
#   kinds:
#   - Pod
#   namespaces:
#   - kube-system
# -- Add preconditions to individual policies.
# Policies with multiple rules can have individual rules excluded
# by using the name of the rule as the key in the `policyPreconditions` map.
policyPreconditions: {}
# # Exclude resources from individual policies
# require-run-as-non-root-user:
# all:
# - key: "{{ request.object.metadata.name }}"
#   operator: NotEquals
#   value: "dcgm-exporter*"
# # Policies with multiple rules can have individual rules excluded
# require-drop-all:
# any:
# - key: "{{ request.object.metadata.name }}"
#   operator: NotEquals
#   value: "dcgm-exporter*"
# adding-capabilities-strict:
# all:
# - key: "{{ request.object.metadata.name }}"
#   operator: NotEquals
#   value: "dcgm-exporter*"
```

Исключения #2

Ресурс Policy Exceptions (alpha)

Можно исключать именно ресурсом в кластере

Можно делать временные исключения с помощью ClusterCleanupPolicy

Создание таких ресурсов надо контролировать:

- RBAC
- Отдельными политиками Kyverno (в доке)
- GitOps approve PR с ресурсами

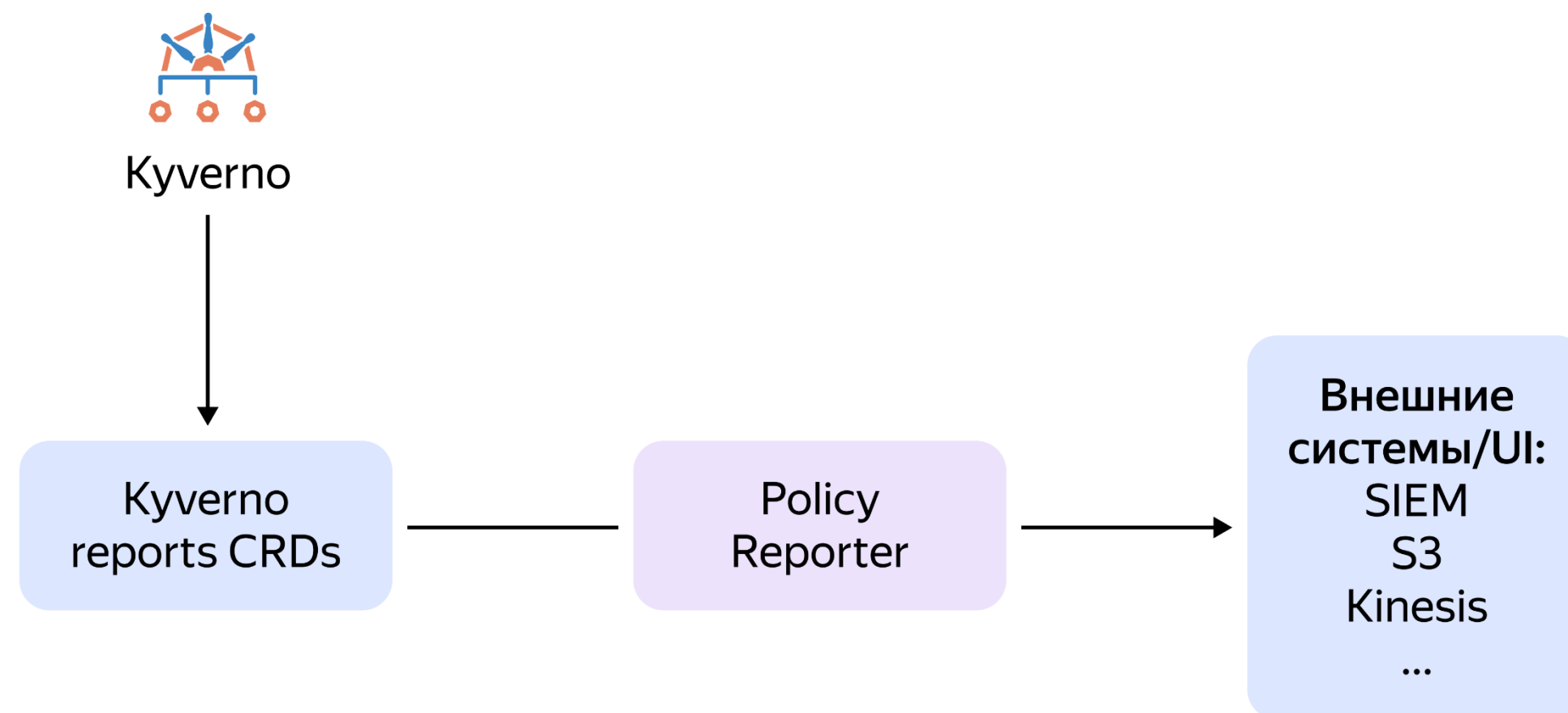


clck.ru/34SJsr

```
apiVersion: kyverno.io/v2alpha1
kind: PolicyException
metadata:
  name: delta-exception
  namespace: delta
spec:
  exceptions:
  - policyName: disallow-host-namespaces
    ruleNames:
    - host-namespaces
    - autogen-host-namespaces
  match:
    any:
    - resources:
        kinds:
        - Pod
        - Deployment
        namespaces:
        - delta
        names:
        - important-tool*
```

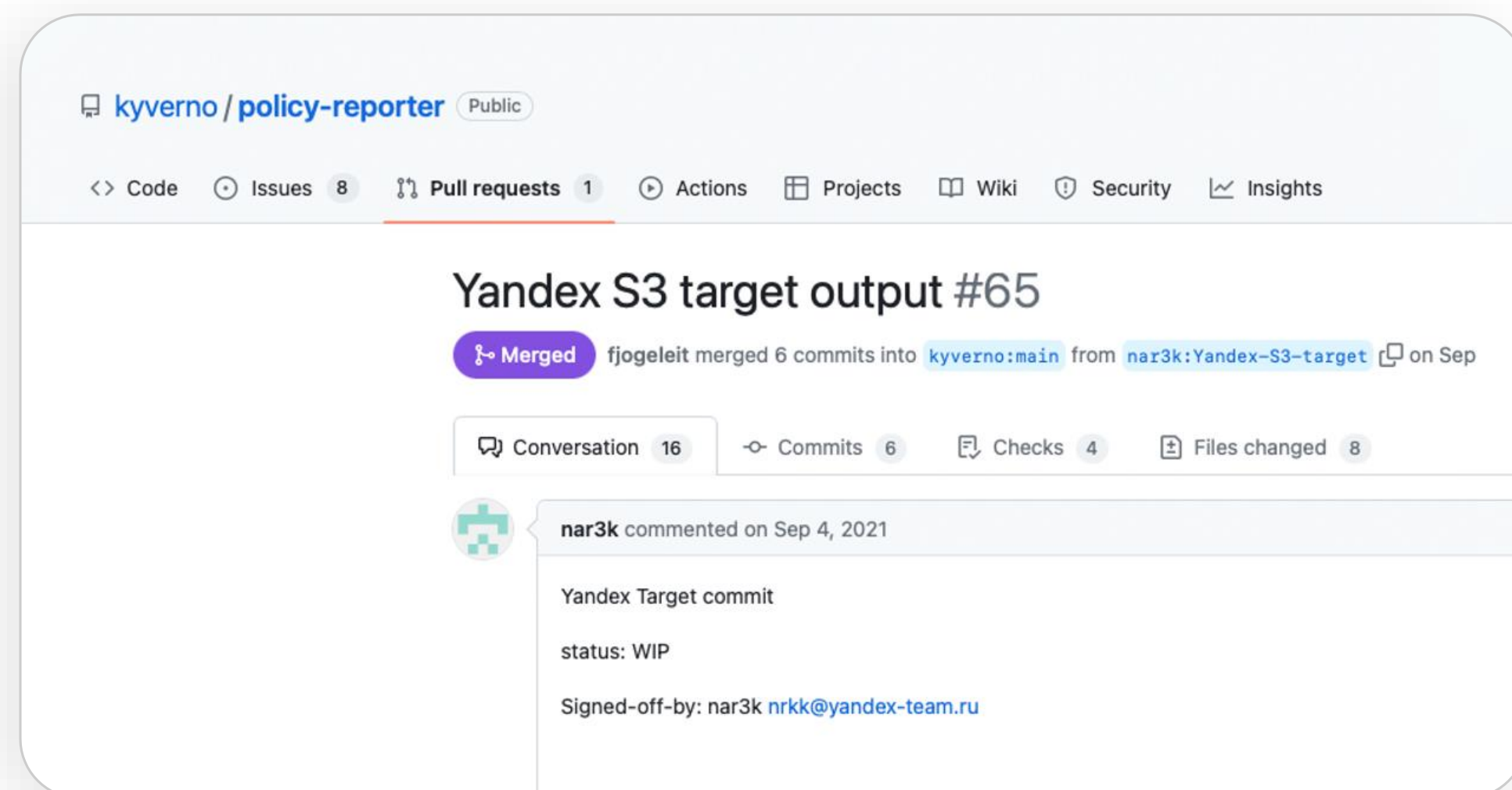
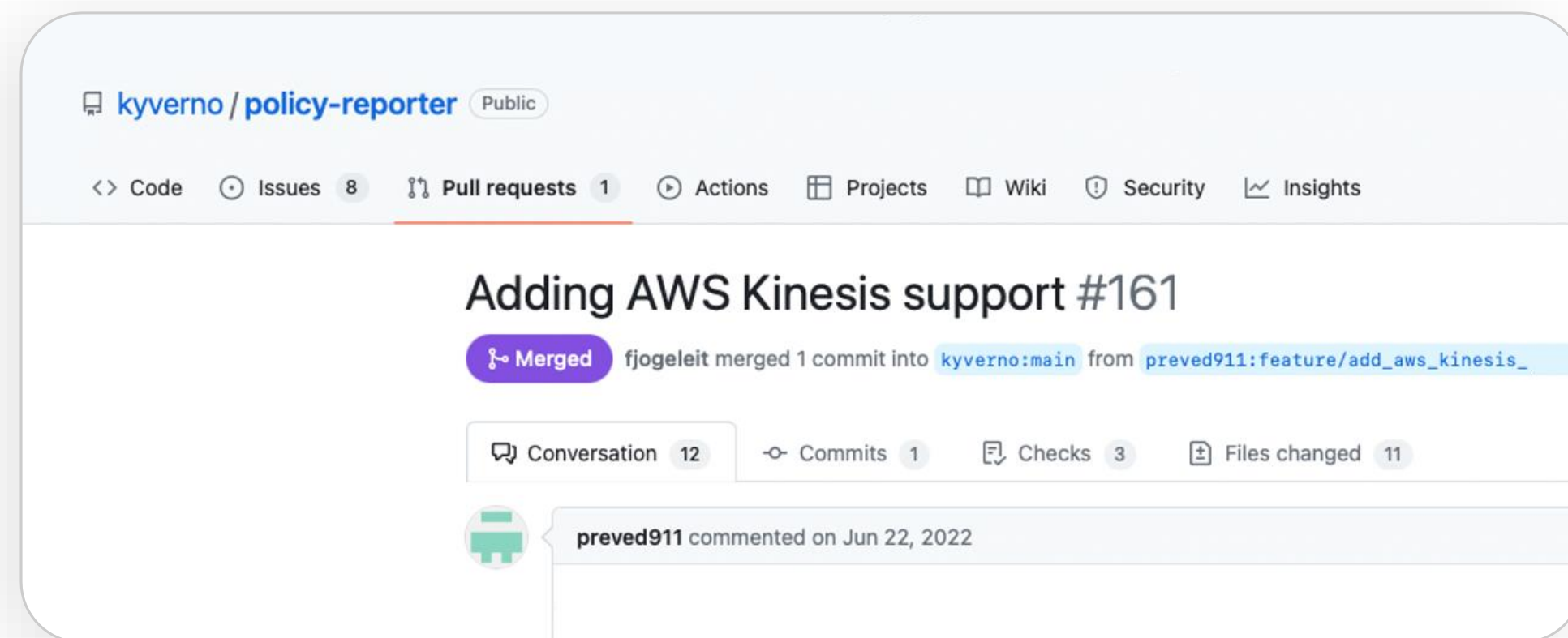
Policy Reporter

Policy Reporter



- Отдельный helm-chart
- Экспортирует алерты Куverno в различные внешние системы
- Можно использовать UI для просмотра
- Формат Reports CRD поддерживает уже kube-bench, Trivy, jsPolicy и Falco

Куда слать?



Поддержано много destinations

- Loki
- Discord
- ELK
- Slack
- Webhook
- UI
- S3
- Kinesis (Yandex YDS)

Что отправляет?

По умолчанию отправляет только **detect (audit mode)**

Если хочется отправлять репорты в режиме **enforce** — включать **kyverno-plugin**

Использовать values:

- `kyvernoPlugin.enabled="true"`
- `kyvernoPlugin.blockReports.enabled="true"`

```
api:
  port: 8080

rest:
  enabled: false

metrics:
  enabled: false

blockReports:
  enabled: false
  eventNamespace: default
  results:
    maxPerReport: 200
    keepOnlyLatest: false
    source: "Kyverno Event"

leaderElection:
  enabled: false
  releaseOnCancel: true
  leaseDuration: 15
  renewDeadline: 10
  retryPeriod: 2
```


Дописывать свои поля

Можно подставлять
свои `customFields: {}`

```
"Policy": "require-run-as-nonroot",
"Rule": "autogen-run-as-non-root",
"Status": "fail",
"Severity": "medium",
"Category": "Pod Security Standards (Restricted)",
"Source": "kyverno",
"Timestamp": "2022-12-08T13:13:15Z",
"Properties": {
  "cluster-id": "catg280p9pumglibjs8n"
},
"Resource": {
  "APIVersion": "apps/v1",
  "Kind": "DaemonSet",
  "Name": "kube-proxy",
  "Namespace": "kube-system",
  "UID": "7663bae7-0750-44b3-a967-9f390580927f"
},
"Priority": "warning",
"Scored": true
}
```


Полнота

Policy Reporter формат

```
"Policy": "require-run-as-nonroot",
"Rule": "autogen-run-as-non-root",
"Status": "fail",
"Severity": "medium",
"Category": "Pod Security Standards (Restricted)",
"Source": "kyverno",
"Timestamp": "2022-12-08T13:13:15Z",
"Properties": {
  "cluster-id": "catg280p9pumglibjs8n"
},
"Resource": {
  "APIVersion": "apps/v1",
  "Kind": "DaemonSet",
  "Name": "kube-proxy",
  "Namespace": "kube-system",
  "UID": "7663bae7-0750-44b3-a967-9f390580927f"
},
"Priority": "warning",
"Scored": true
```

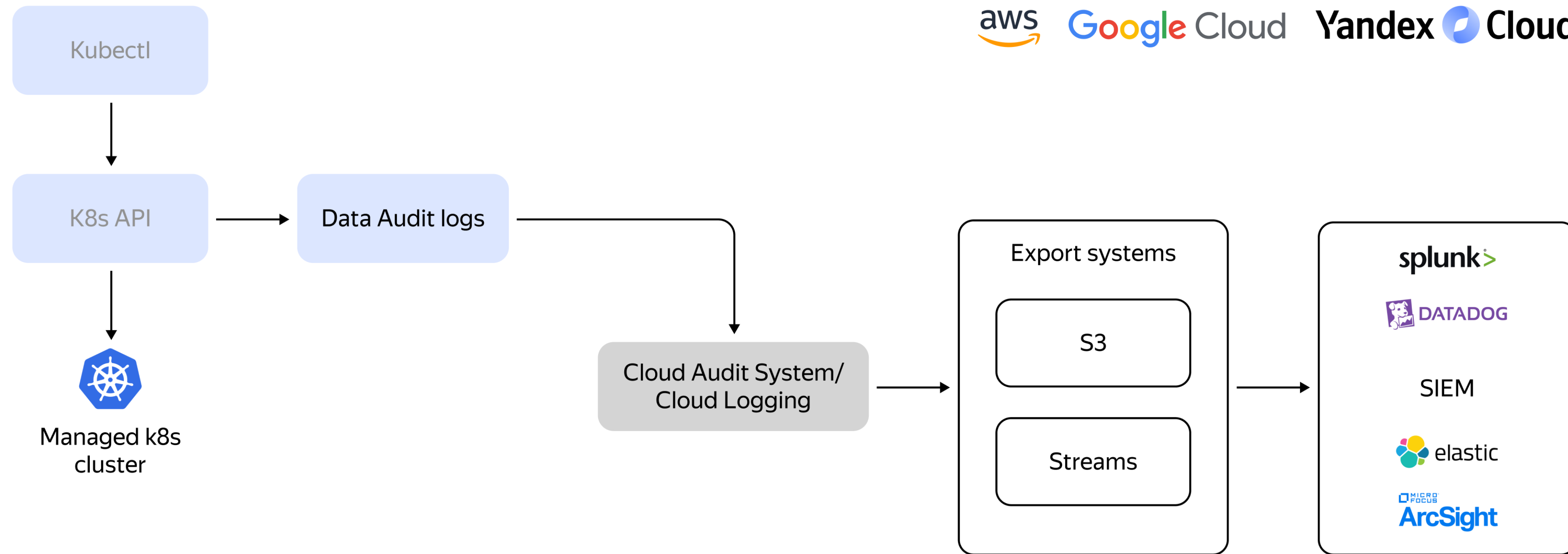
Audit Logs формат (видим только enforce)

```
{
  "level": "RequestResponse",
  "auditID": "709b6676-9a99-41c4-9087-6bba2c3d7602",
  "stage": "ResponseStarted",
  "requestURI": "/api/v1/namespaces/default/pods/pod/exec?
  command=sh&container=pod&stdin=true&stdout=true&tty=true",
  "verb": "create",
  "user": {
    "username": "ajesnkfk771bh50isvg",
    "uid": "ajesnkfk771bh50isvg",
    "groups": [2]
  },
  "sourceIPs": [
    "5.255.223.122"
  ],
  "userAgent": "kubectl/v1.23.4 (darwin/amd64)
  kubernetes/e6c093d",
  "objectRef": {
    "resource": "pods",
    "namespace": "default",
    "name": "pod",
    "apiVersion": "v1",
    "subresource": "exec"
  },
  "responseObject": {
    "kind": "Status",
    "apiVersion": "v1",
    "metadata": {
```

1. Нюансы настройки
2. Audit logs. На что реагировать
3. А в какую сторону двигаться дальше?

Облако

aws Google Cloud Yandex Cloud



На что реагировать?

~2 ГБ в день

лёт один пустой
K8s-кластер

В bare metal можно тюнить политику

В облаках обычно default
«по максимуму»

Файл поликити аудита Google Cloud:
<https://clck.ru/34aLbh>



Use cases K8s



clck.ru/34SLcN

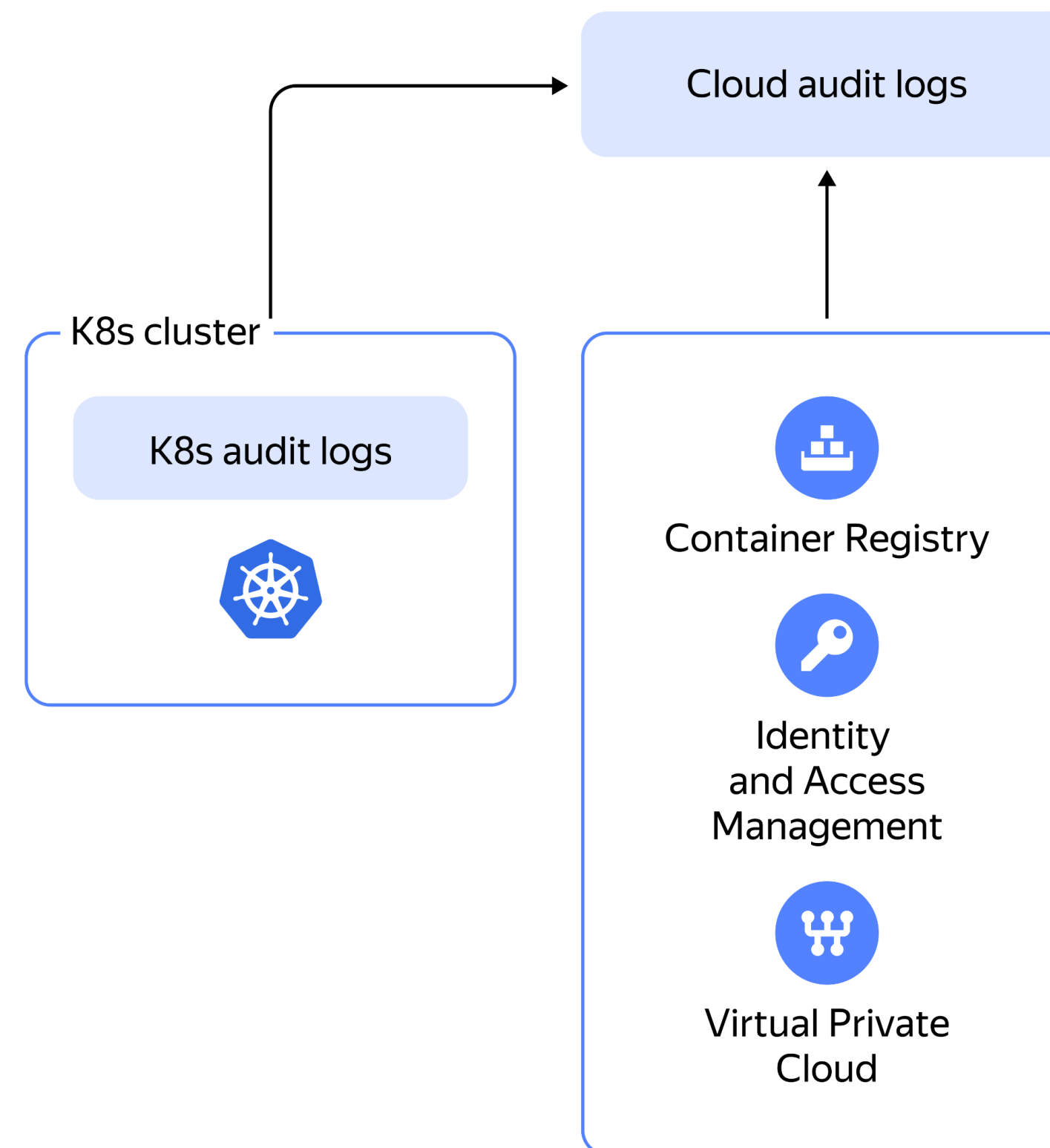
Набор интересных событий безопасности в журналах аудита K8s

Название	Запрос на языке ELK
Событие срабатывания Куверно в режиме блокировки	filter "\$.responseObject.status" = 'Failure' and \$.responseObject.message" LIKE '%deny-exec-by-pod-and-container%'; (название политики меняем под свои политики)
События запрещены в доступе — неавторизованные	event.dataset : yandexcloud.k8s_audit_logs и responseStatus.reason : Forbidden, а не user.name : (системный узел или <i>привратник</i> , или <i>куверно</i> , или <i>прокси</i> , или <i>планировщик</i> , или <i>анонимный</i> , или <i>csi</i> , или <i>контроллер</i>)
Назначение cluster-admin или роль администратора (clusterrolebinding или rolebinding)	event.dataset: yandexcloud.k8s_audit_logs и requestObject.roleRef.name.keyword:(cluster-admin или admin) и objectRef.resource.keyword: (clusterrolebindings или rolebindings) и verb: создать, а не responseObject.reason: уже существует
Успешное подключение к кластеру с внешним IP-адресом	event.dataset : yandexcloud.k8s_audit_logs и source.ip : * а не responseStatus.status : Ошибка
NetworkPolicies: создание, удаление, изменение (Cilium)	event.dataset: yandexcloud.k8s_audit_logs и requestObject.kind.keyword: (NetworkPolicy или CiliumNetworkPolicy или DeleteOptions) и verb: (создать, обновить или удалить) и objectRef.resource: networkpolicies
Еxec входного контейнера (шелл входного контейнера)	event.dataset: yandexcloud.k8s_audit_logs и objectRef.subresource.keyword: exec
Добавить про /port-forward/proxy	event.dataset: yandexcloud.k8s_audit_logs и objectRef.subresource.keyword: portforward
Создание пода с образом НЕ из реестра контейнеров Яндекса	event.dataset : yandexcloud.k8s_audit_logs а не requestObject.status.containerStatuses.image.keyword: <i>cr.yandex/</i> и requestObject.status.containerStatuses.containerID : <i>docker</i> and verb : patch а не requestObject.status.containerStatuses.image.keyword: (<i>falco</i> или <i>openpolicyagent</i> или <i>kuverno</i> или <i>k8s.gcr.io</i>)
Создание пода в пространстве имён kube-system	event.dataset : yandexcloud.k8s_audit_logs и objectRef.namespace.keyword: kube-system и verb : create и objectRef.resource.keyword: requestObject.subresource.keyword: (<i>pod</i> или <i>podtemplate</i>)

А что за пределами K8s audit logs?

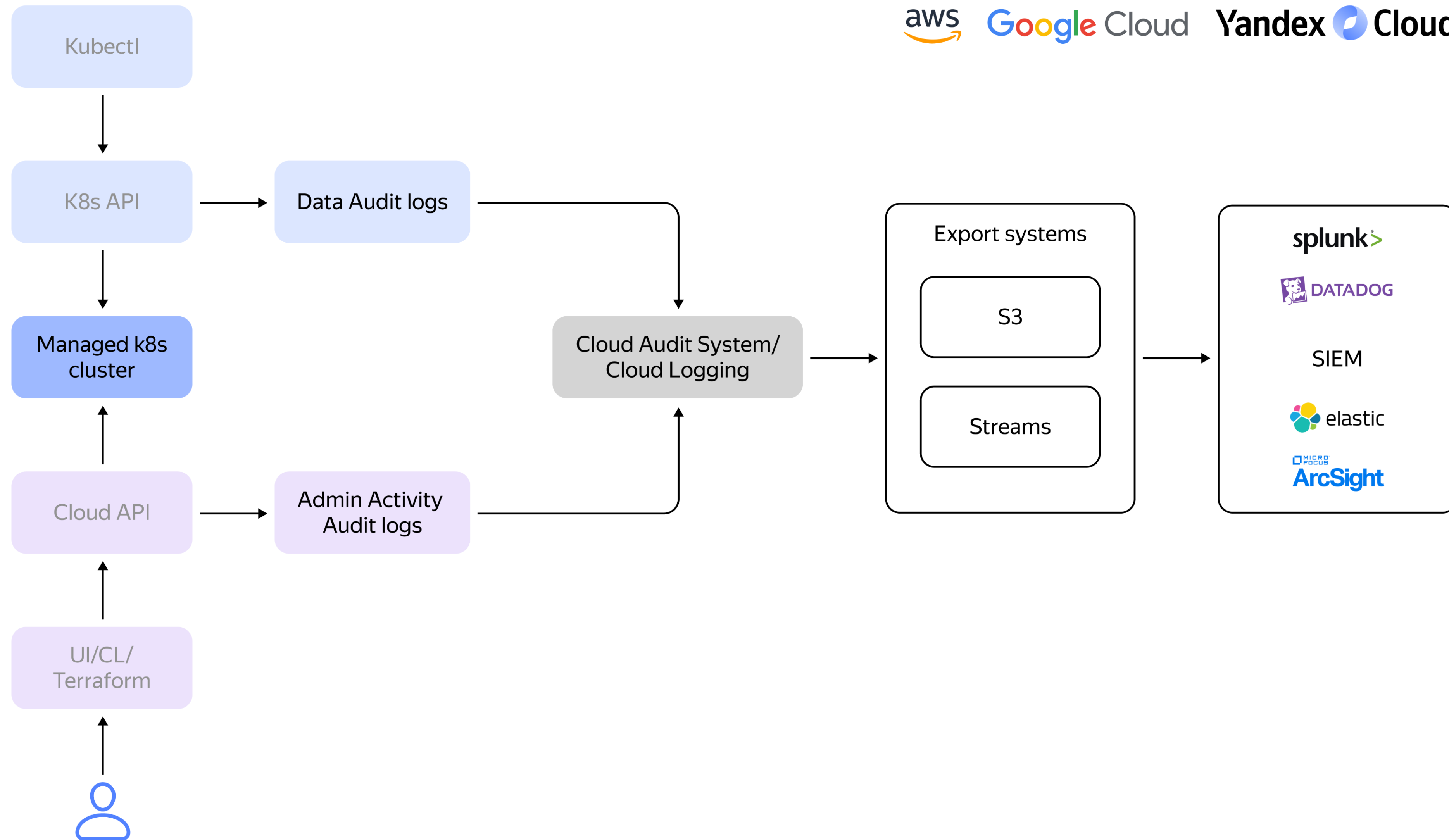
Сам объект кластера
и объекты вокруг (admin
activity/control plane)

Также пишут события
безопасности



Облако

aws Google Cloud Yandex Cloud



Use cases K8s — Audit Trails

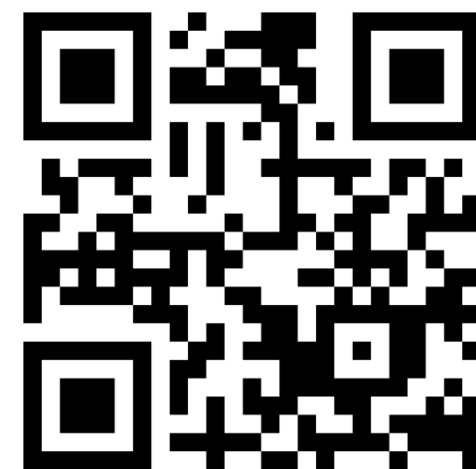


clck.ru/XJwk7

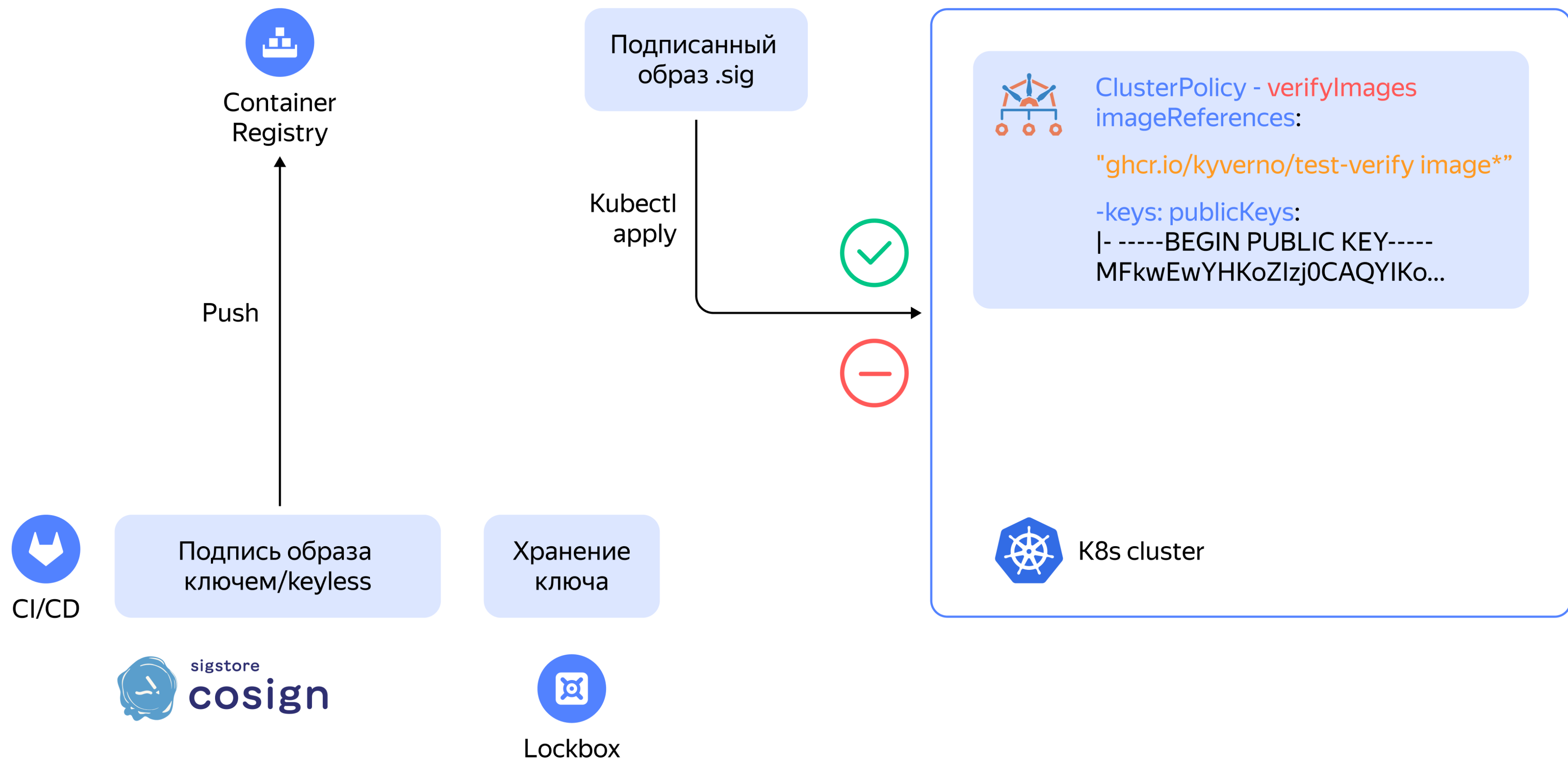
New Не назначена SG на мастер	<code>json_payload.event_type: "yandex. cloud.audit.k8s.CreateCluster"</code> <code>and not json_payload.request_parameters.master_spec.security_group_ids EXISTS</code>
New Кластер имеет публичный адрес	<code>json_payload.event_type: "yandex. cloud.audit.k8s.CreateCluster"</code> <code>and json_payload.request_parameters.master_spec.zonal_master_spec.external_v4_address_spec.address EXISTS</code>
New Не включено автоматическое обновление для Kubernetes master	<code>json_payload.event_type: "yandex.cloud.audit. k8s.CreateCluster"</code> <code>and not json_payload.request_parameters. master_spec.maintenance_policy.auto_upgrade EXISTS</code>
New Не включено автоматическое обновление Kubernetes node	<code>json_payload.event_type : "yandex. cloud.audit.k8s.CreateNodeGroup "</code> <code>and not json_payload. request_parameters. mainten ance_policy.auto_upgrade = "true"</code>
New Не включено шифрование на KMS-ключе etcd базы	<code>json_payload.event_type : "yandex. cloud. audit.k8s.CreateCluster"</code> <code>and not json_payload.request_parameters. kms_pro vider. key_id exists</code>
New Не включена network policy либо cilium на уровне кластера	<code>json_payload.event_type : "yandex. cloud.audit. k8s. CreateCluster"</code> <code>and not json_payload.request_parameters. network_policy.provider exists</code>

1. Нюансы настройки
2. Audit logs. На что реагировать
3. А в какую сторону двигаться дальше?

Kyverno Verify Images



clck.ru/34SSRL



Проверка содержания in-to-to attestations (SLSA)

Можно проверять любые
поля аттестации.

Из интересных готовых политик:

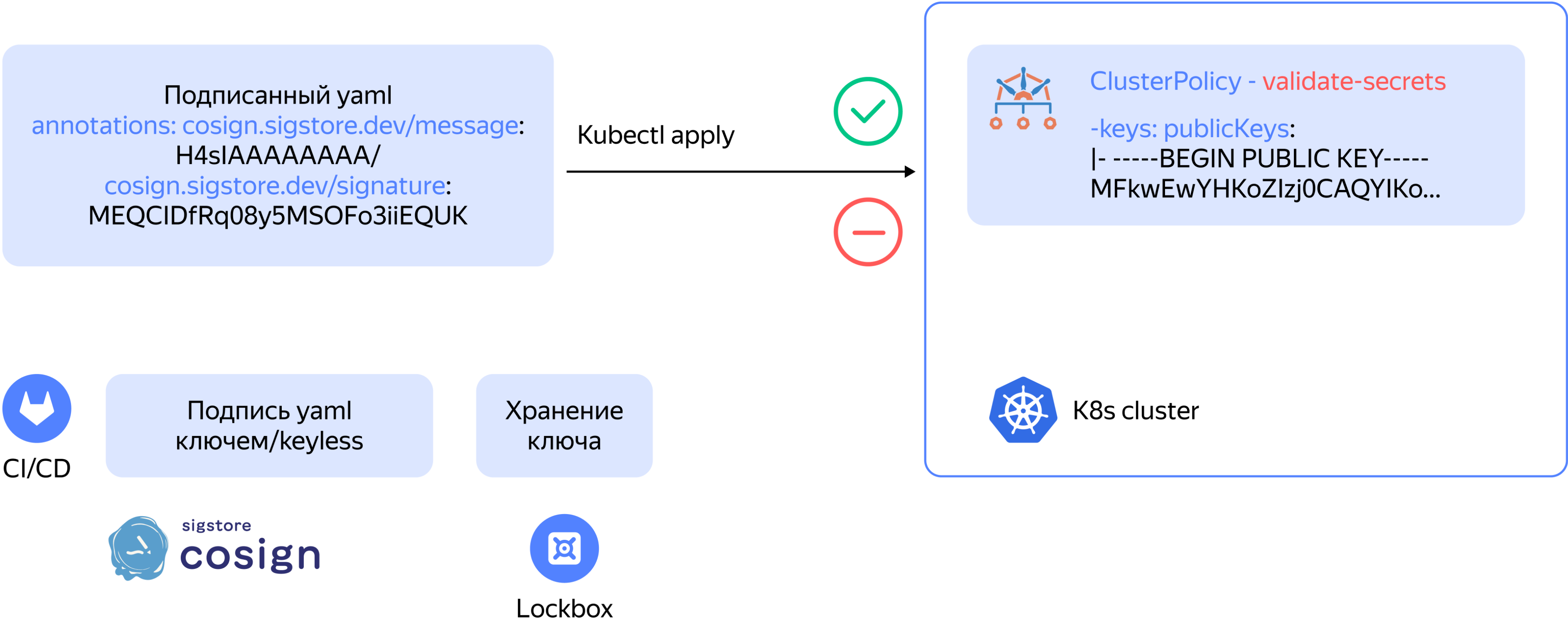
- Require Image Vulnerability Scans
(поле даты последнего скана)
- Verify Image Check CVE-2022-42889
(поля sbom)
- Verify CycloneDX SBOM
(Keyless)

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: attest-code-review
spec:
  validationFailureAction: Enforce
  background: false
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
  rules:
    - name: attest
      match:
        any:
          - resources:
              kinds:
                - Pod
      verifyImages:
        - imageReferences:
            - "registry.io/org/app*"
          attestations:
            - predicateType: https://example.com/CodeReview/v1
              attestors:
                - entries:
                    - keys:
                        publicKey: |-
                          -----BEGIN PUBLIC KEY-----
                          MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEzDB0FiCzAWf/BhHLpikFs6p853/G
                          3A/jt+GFb0Jjpn7vJyb28x4XnR1M5pwUUcpzIZkIgSsd+XcTnrBPVoiyw==
                          -----END PUBLIC KEY-----
              conditions:
                - all:
                    - key: "{{ repo.uri }}"
                      operator: Equals
                      value: "https://git-repo.com/org/app"
                    - key: "{{ repo.branch }}"
                      operator: Equals
                      value: "main"
                    - key: "{{ reviewers }}"
                      operator: In
                      value: ["ana@example.com", "bob@example.com"]
```

Подпись YAML манифестов



clck.ru/34SSRL



7 июня 2023 📍 Москва, МЦК ЗИЛ

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред



Contacts:

Email:

Twitter:

Tg: @alexwee

Site:

Буду рад продолжить общение



Алексей Миртов

Руководитель группы продуктовой
архитектуры Security & Compliance