Защищаем Kubernetes при помощи StackRox — дешево, сердито, эффективно?

Георг Гаал

Кто я такой

- ведущий инженер Zodia Markets
- администратор русскоязычных tg каналов по kubernetes, gitlab, gitops etc.
- участник ПК различных конференций
- пишу статьи :-)

Гипотетическая ситуация

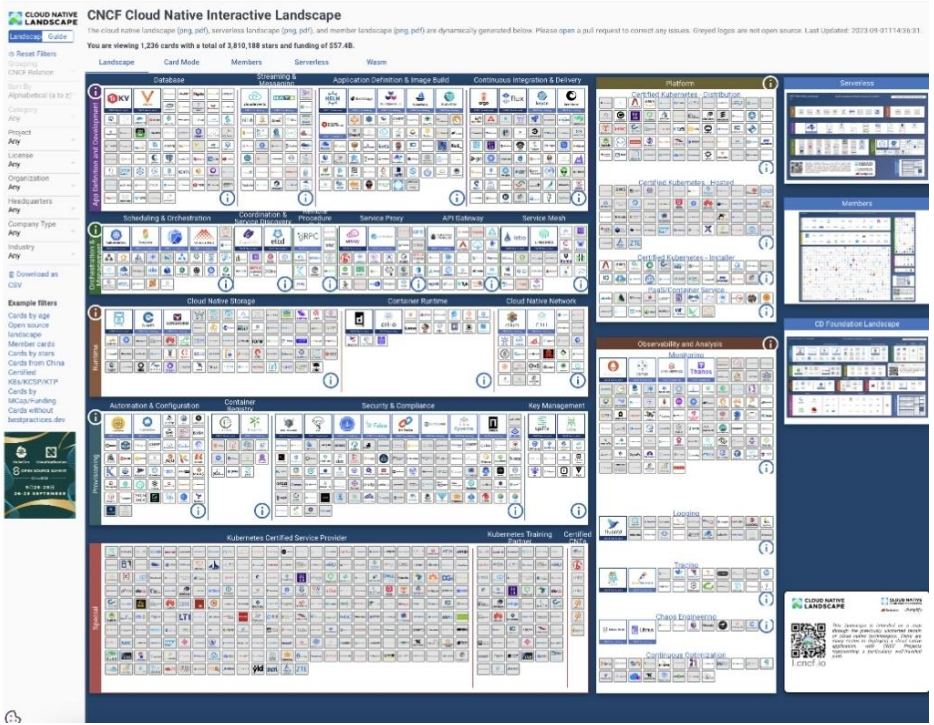
DevOops

- Мы стартап
- Мы поехали в облако и развернули k8s
- Пустили трафик
- ...
- Всё хорошо
- ...
- А теперь непонятно
- Что делать? Кто виноват

Что есть на рынке

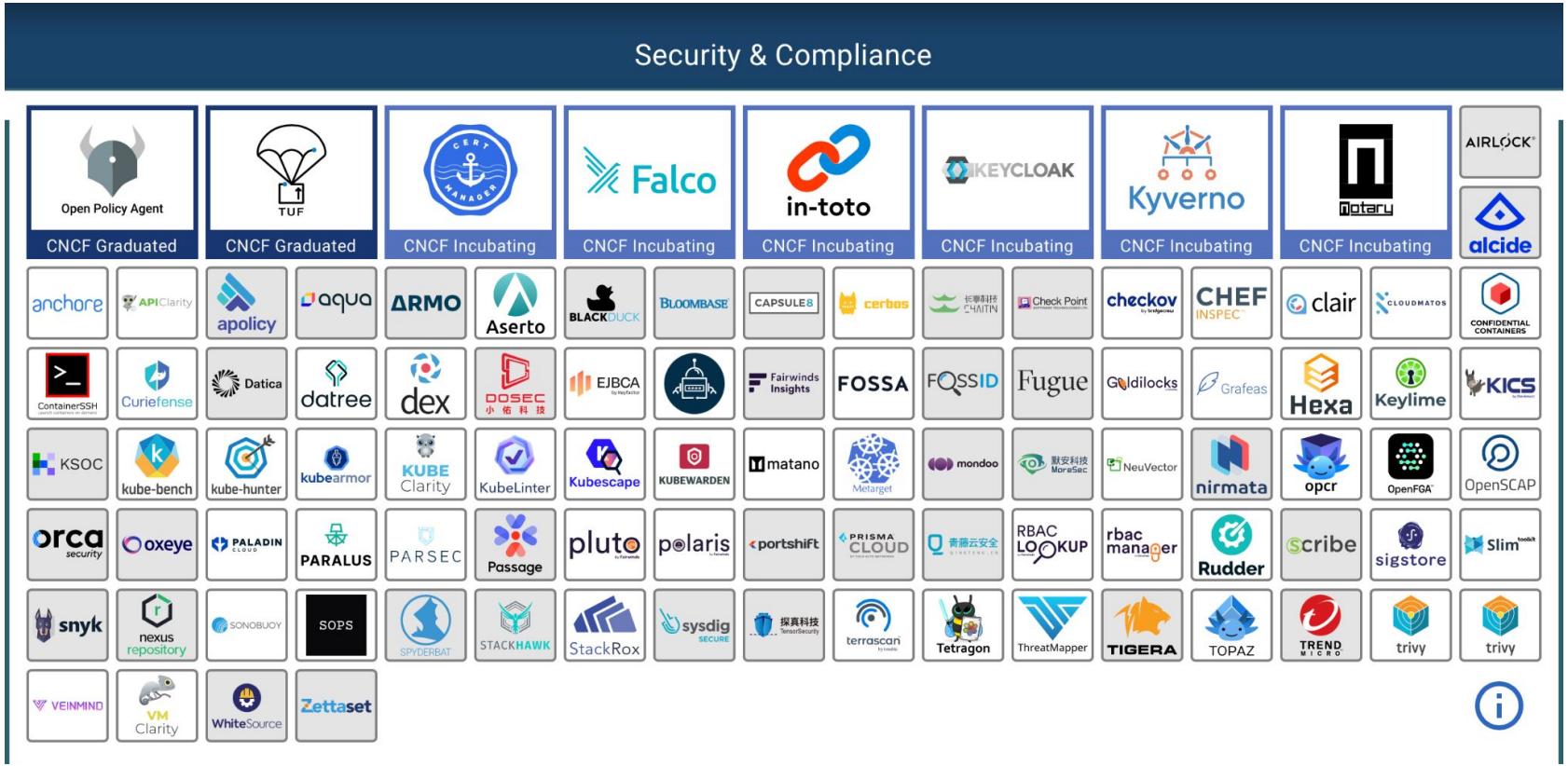
DevOops

https://landscape.cncf.io



Что есть на рынке

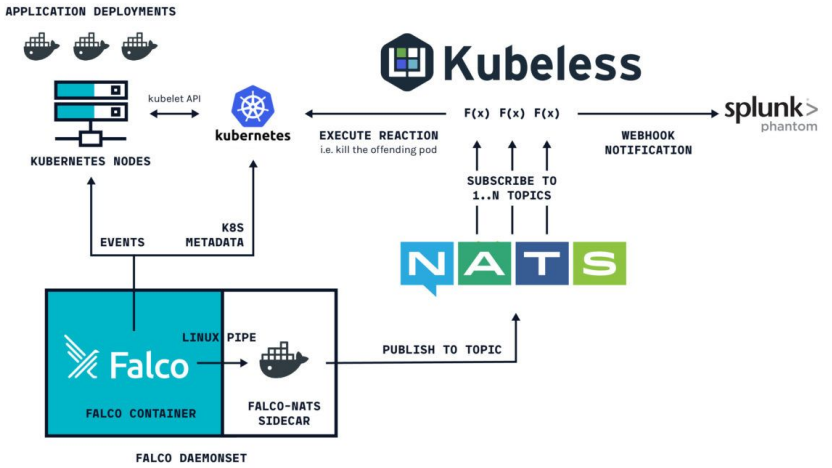
DevOops



Что есть на рынке

- https://github.com/falcosecurity/falco
- k8s native (helm + daemonset)
- умеет собирать события с узла
- умеет собирать события аудита k8s api
- нет реакции на события (!!!)
- rule-based - поэтому легко обходится (!!!)
- нет контекста
- см. https://github.com/draios/sysdig и https://github.com/draios/sysdig-inspect

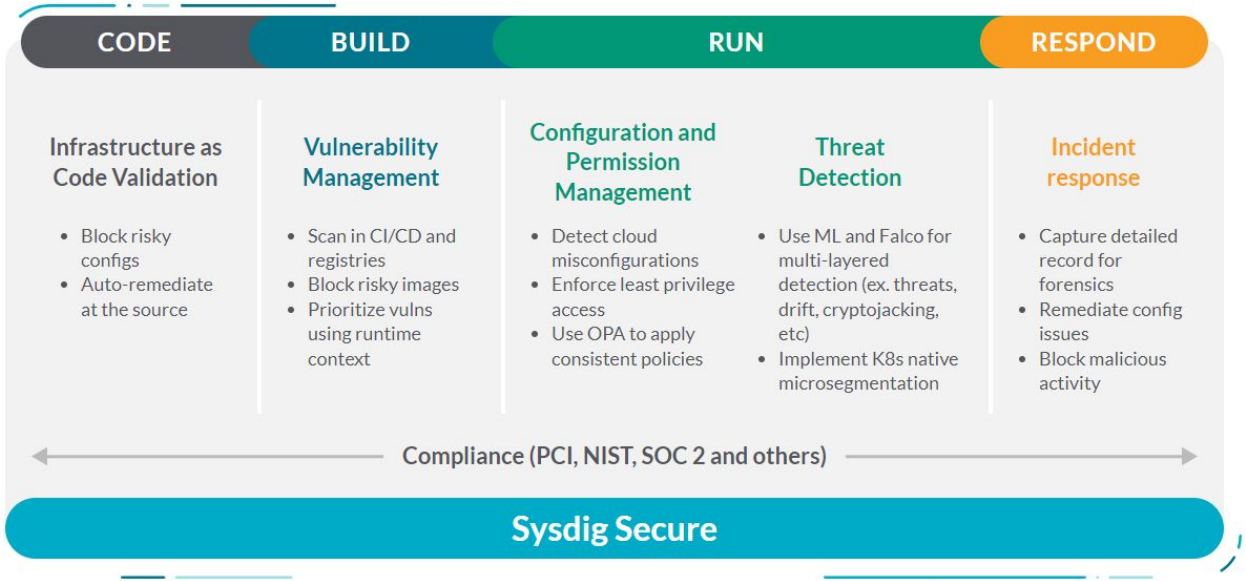
Falco



DevOops

Что есть на рынке

На базе falco сделан платный SysDig Secure
https://sysdig.com/



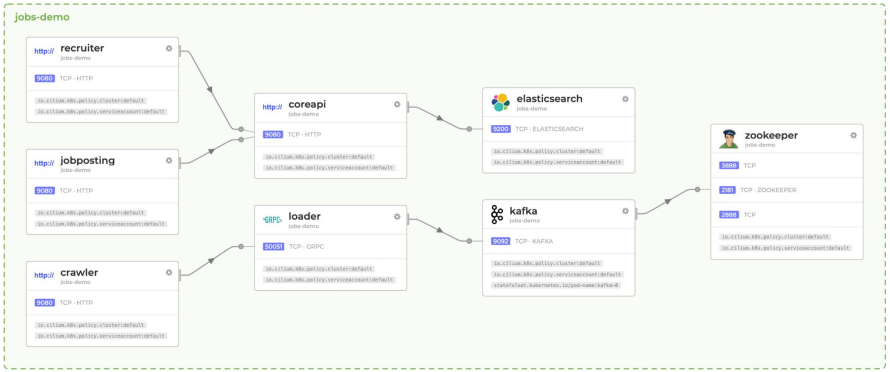
Что есть на рынке

Tetragon

- https://github.com/cilium/tetragon
- k8s native
- нетривиален в настройке
- только лишь агент сбора
- Cilium ONLY

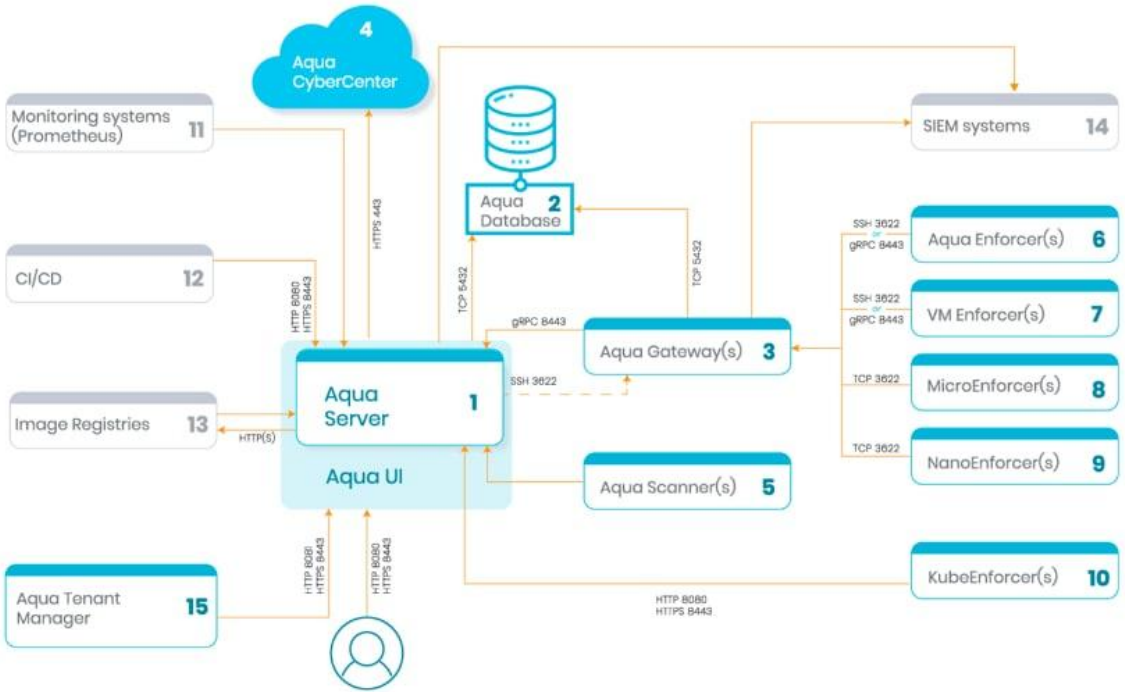
зато с Cilium у нас есть Hubble!

Hubble



Что есть на рынке

Aqua Security



DevOops

Что есть на рынке

kube-bench

- https://github.com/aquasecurity/kube-bench
- Сканирование на CIS compliance

kube-hunter

- https://github.com/aquasecurity/kube-hunter
- агрессивное сканирование на уязвимости

Что есть на рынке

куча различных сканеров образов

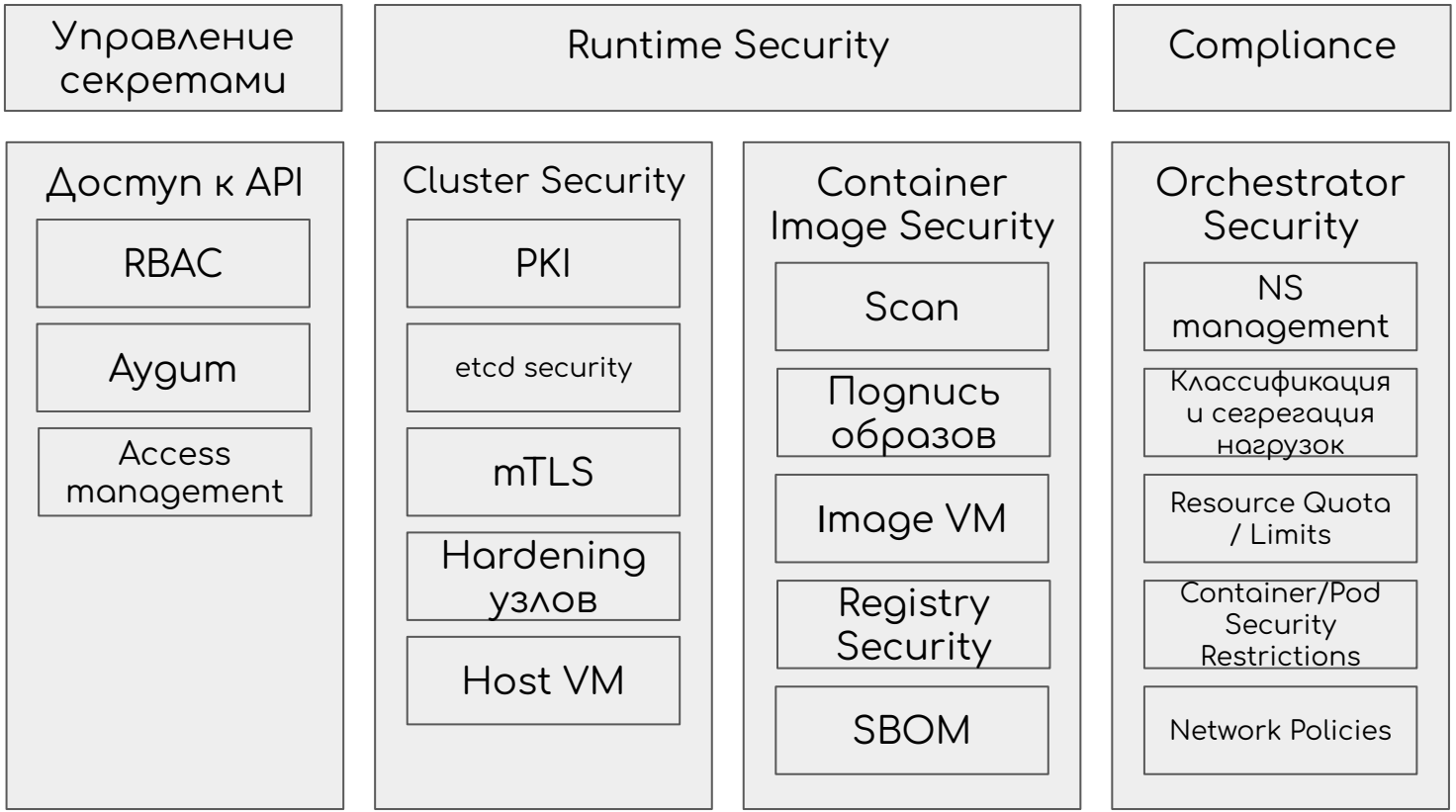
https://github.com/quay/clair

https://github.com/aquasecurity/trivy

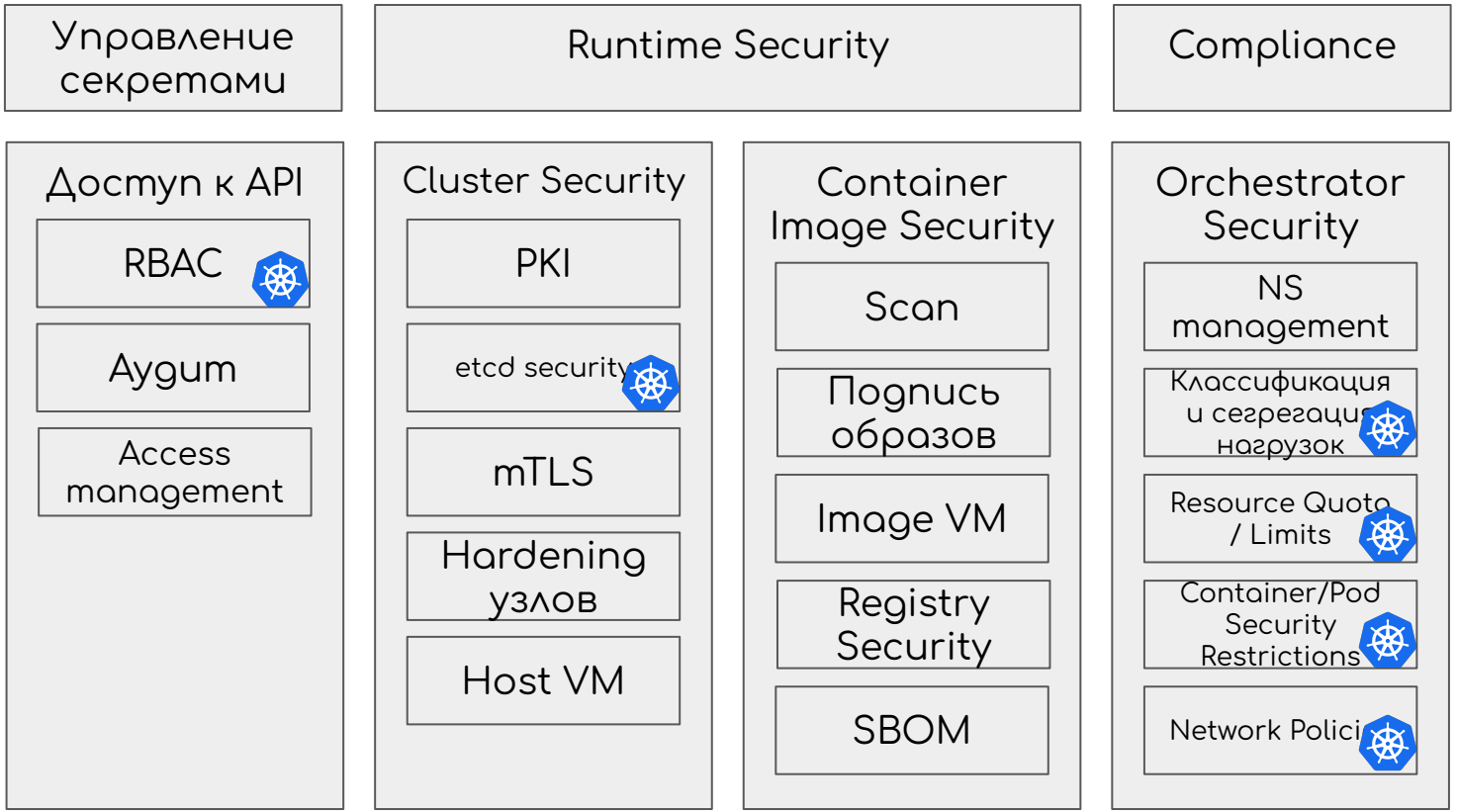
https://github.com/anchore/anchore-engine
(deprecated)

DevOops

Безопасность kubernetes



Безопасность kubernetes



Безопасность kubernetes

DevOops

Управление секретами

Runtime Security

Compliance

Доступ к API

- RBAC
- Aygum
- Access management

Cluster Security

- PKI
- etcd security
- mTLS
- Hardening узлов
- Host VM

Container Image Security

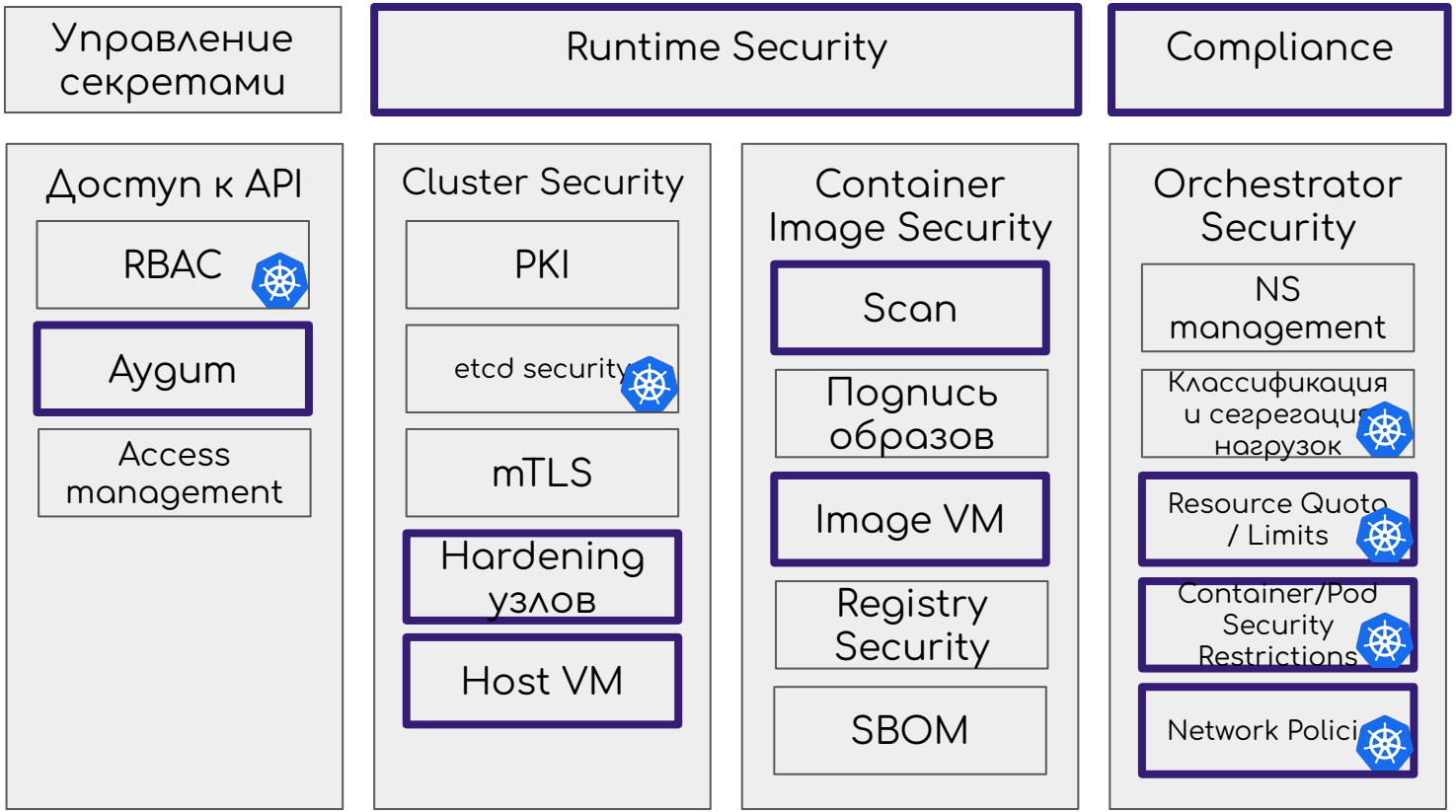
- Scan clair
- Подпись образов
- Image VM
- Registry Security
- SBOM

Orchestrator Security

- NS management
- Классификация и сегрегация нагрузок
- Resource Quota / Limits
- Container/Pod Security Restrictions
- Network Polici

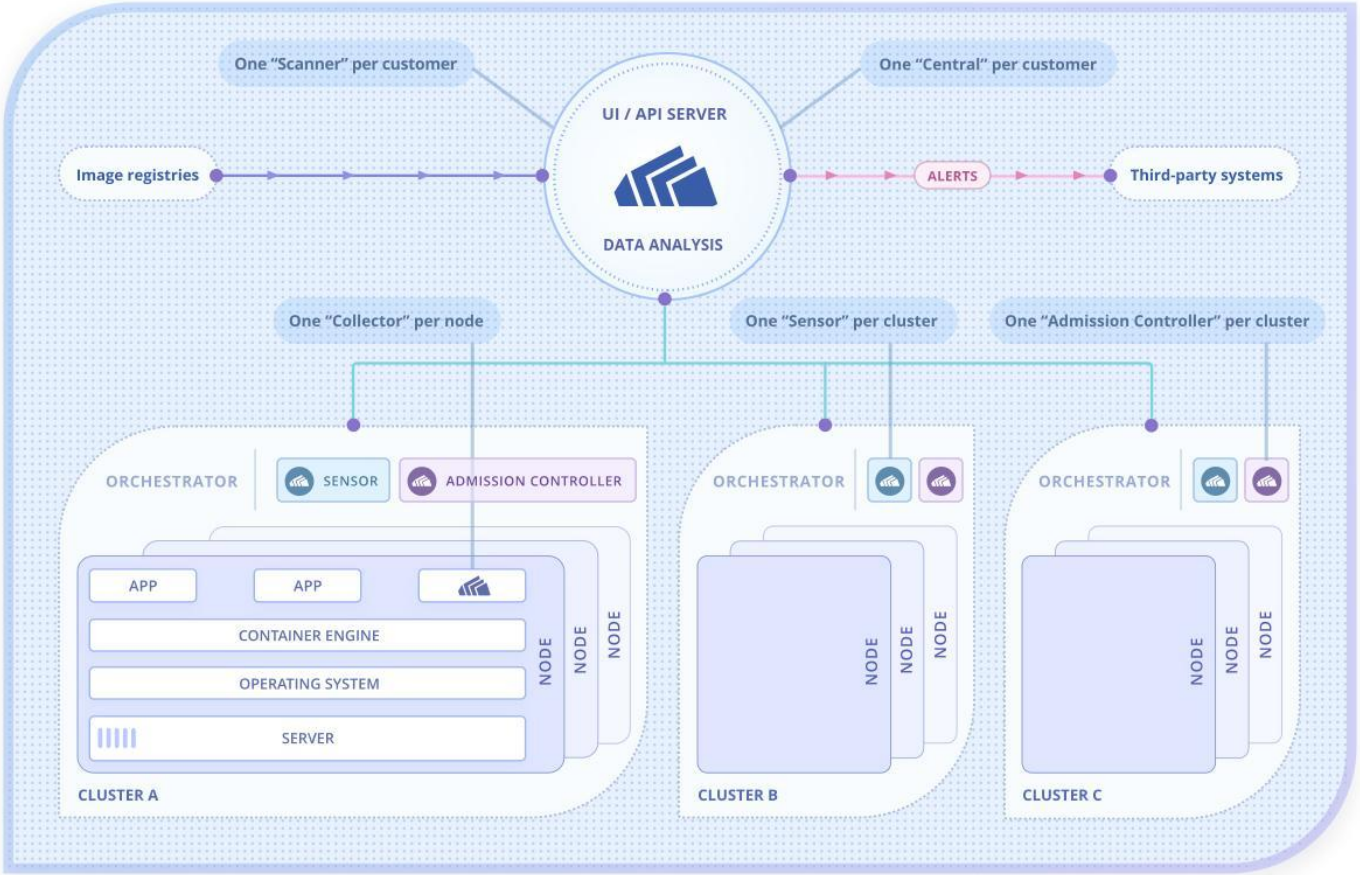
Безопасность kubernetes

StackRox



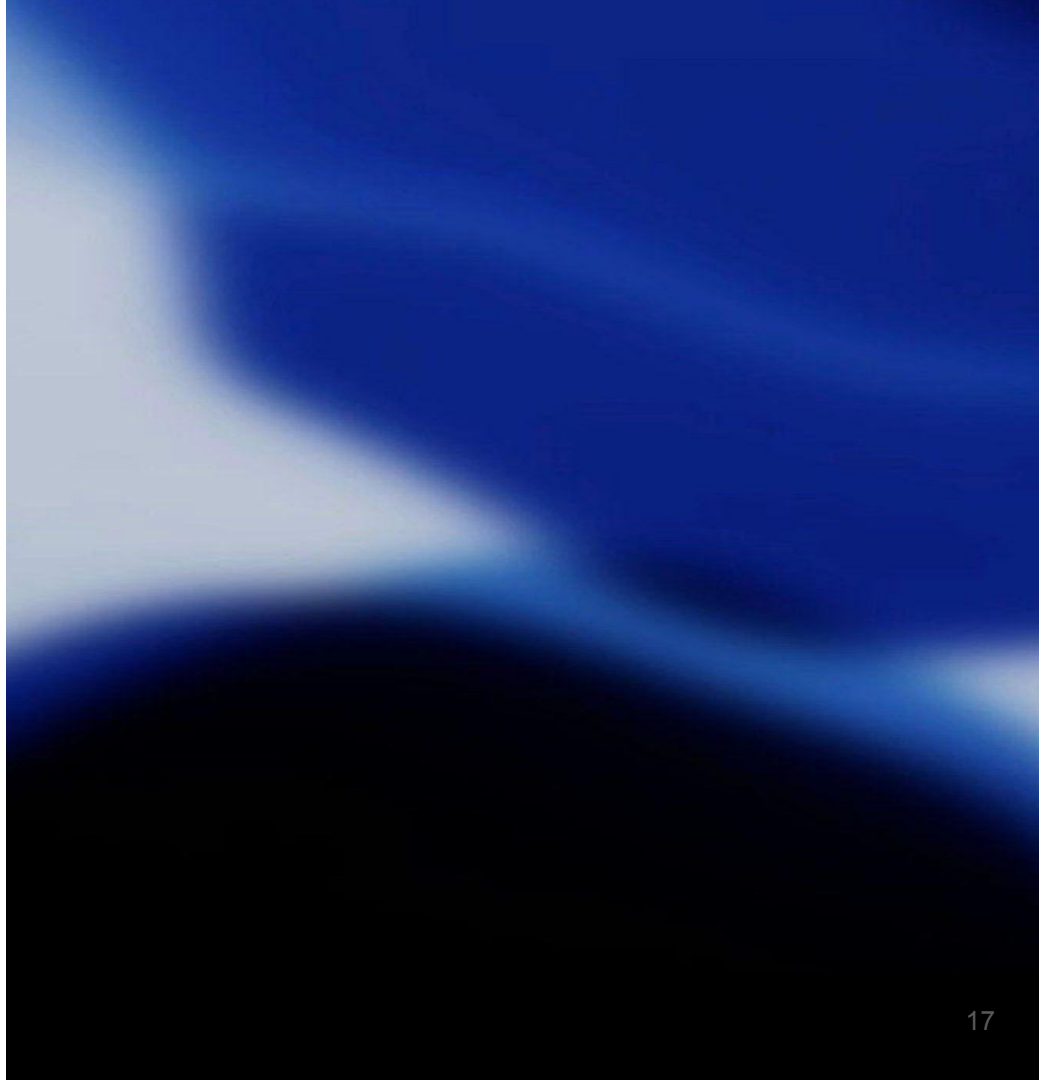
Архитектура StackRox

DevOops



Установка

1. устанавливаем component central
2. устанавливаем agent'ы (sensor)
3. настраиваем интеграции
4. настраиваем уведомления



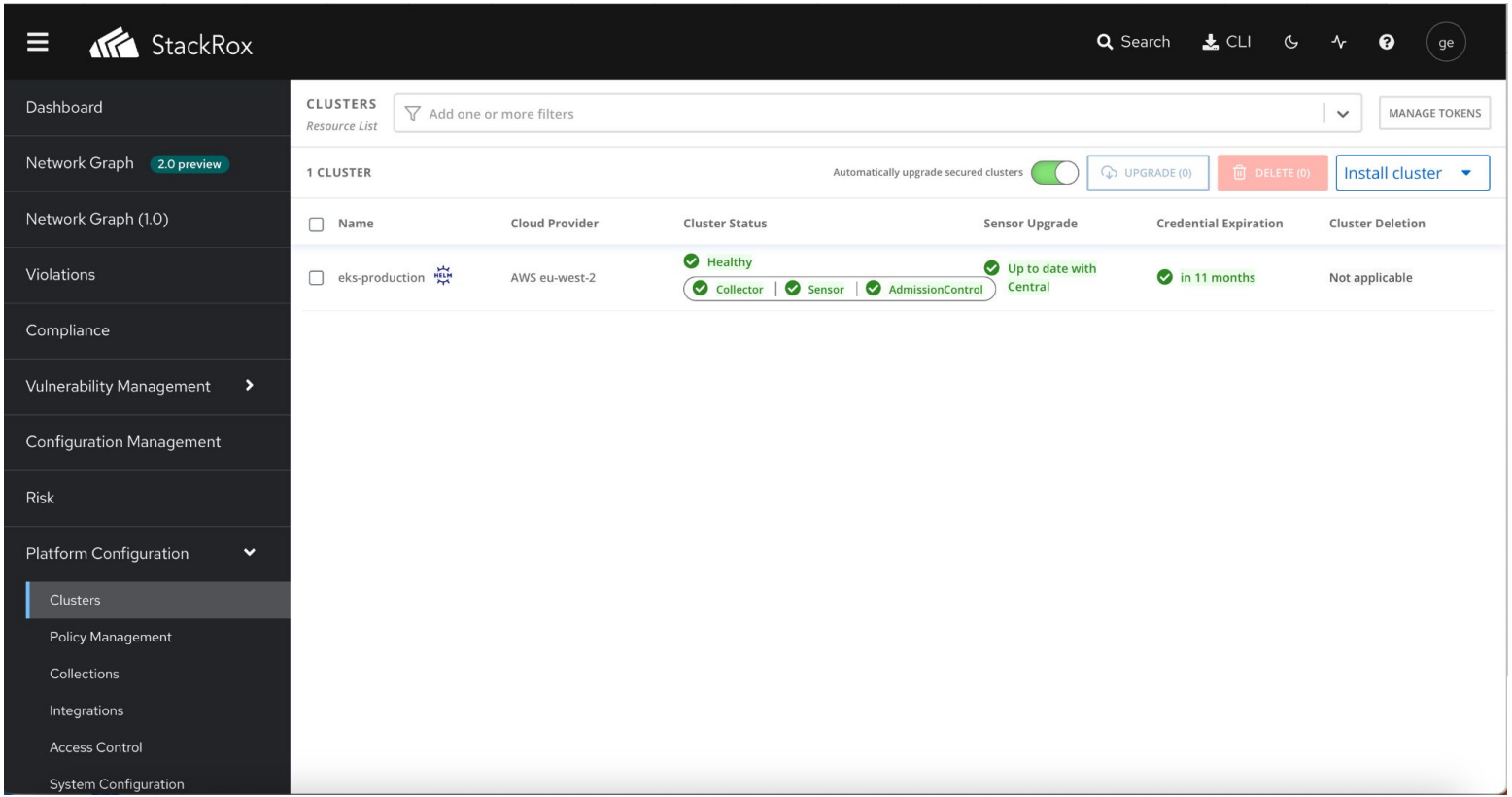
Установка central

DevOops

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: stackrox
  annotations:
    openshift.io/requester: system
---
apiVersion: source.toolkit.fluxcd.io/v1beta1
kind: HelmRepository
metadata:
  name: stackrox
  namespace: stackrox
spec:
  interval: 1m0s
  timeout: 1m0s
  url: https://mirror.openshift.com/pub/rhacs/charts
---
apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: stackrox-central-services
  namespace: stackrox
spec:
  install:
    remediation:
      retries: 3
  upgrade:
    remediation:
      retries: 3
  releaseName: stackrox-central-services
  chart:
    spec:
      chart: stackrox-central-services
      sourceRef:
        kind: HelmRepository
        name: stackrox
      version: '74.1.0'
  targetNamespace: stackrox
  interval: 1m0s
  values:
    env:
      offlineMode: false
    imagePullSecrets:
      useExisting: []
      allowNone: true
```

```yaml
central:
  db:
    image:
      registry: quay.io/stackrox-io
      name: central-db
      tag: 3.74.1
    enabled: true
    external: false
    persistence:
      persistentVolumeClaim:
        claimName: "central-db"
        size: "10Gi"
        storageClass: "gp2"
        createClaim: true
  adminPassword: #подставить свои пароли
    htpasswd: |
      admin:$2y$05$5sd5ZuAD3bCX9ddhokQhS.2zLRisC2ZeLFXi/meQ.WZi5ykxrLZRm
      georg:$2y$05$WnbMo0H0aZLZJaQ9bHd3TOirRpzw/YA1Fl6YmxmFw1luweAQLw.bW
  image:
    registry: quay.io/stackrox-io
    name: main
    tag: 3.74.1
  disableTelemetry: true
  persistence:
    persistentVolumeClaim:
      claimName: "stackrox-db"
      size: "10Gi"
      storageClass: "gp2"
      createClaim: true
  exposure:
    nodePort:
      enabled: true
scanner:
  dbPassword:
    value: QxY4bVYPHgTzBYLO4Nb28ywS8 # подставить свой пароль
  disable: false
  image:
    registry: quay.io/stackrox-io
    name: scanner
    tag: 3.74.1
  dbImage:
    registry: quay.io/stackrox-io
    name: scanner-db
    tag: 3.74.1
```

Интерфейс

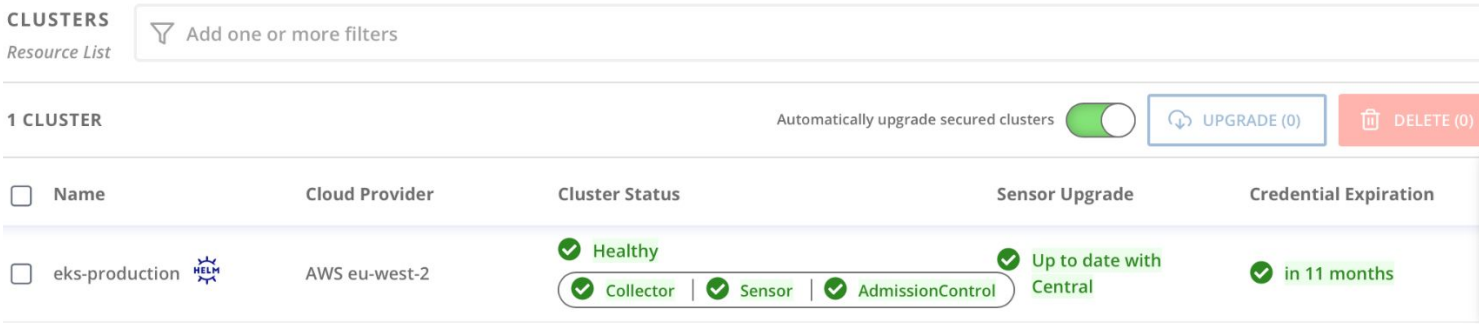


DevOops

DevOops

Установка sensor

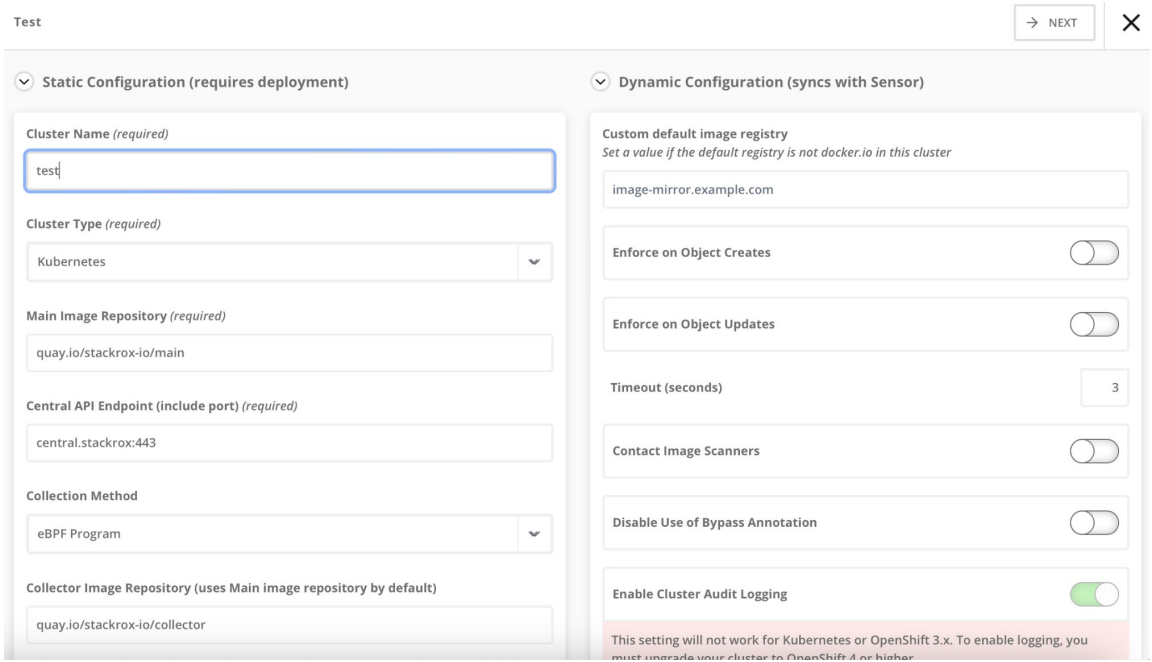
Заходим в список кластеров и выбираем “New Cluster”



DevOops

Установка sensor

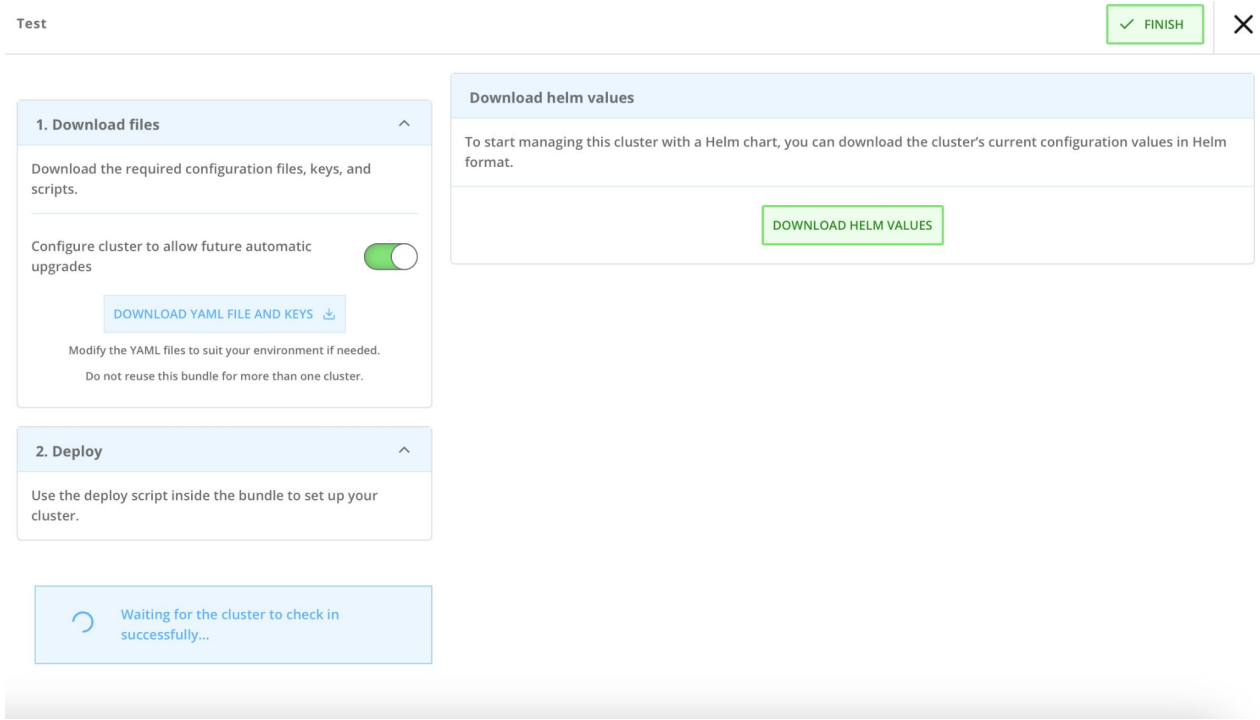
Выбираем опции



DevOops

Установка sensor

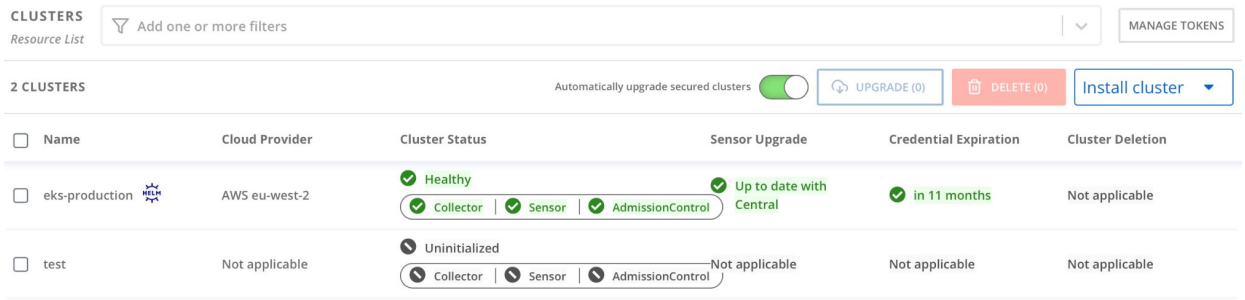
Скачиваем bundle



DevOops

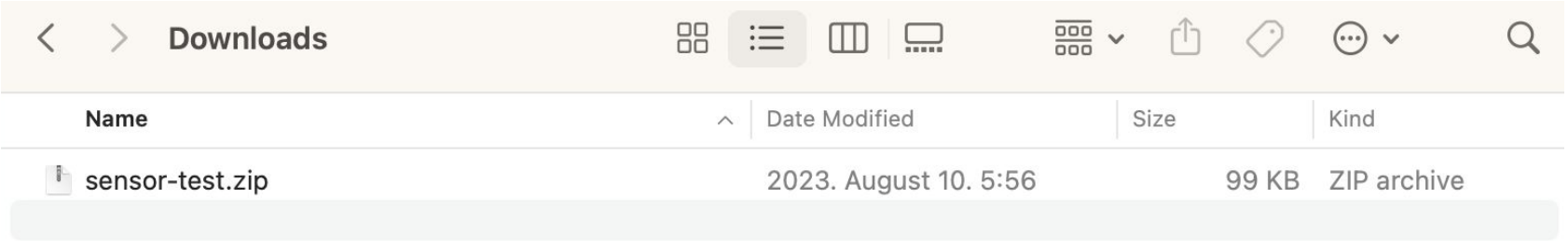
Установка sensor

Кластер переходит в “not applicable” состояние



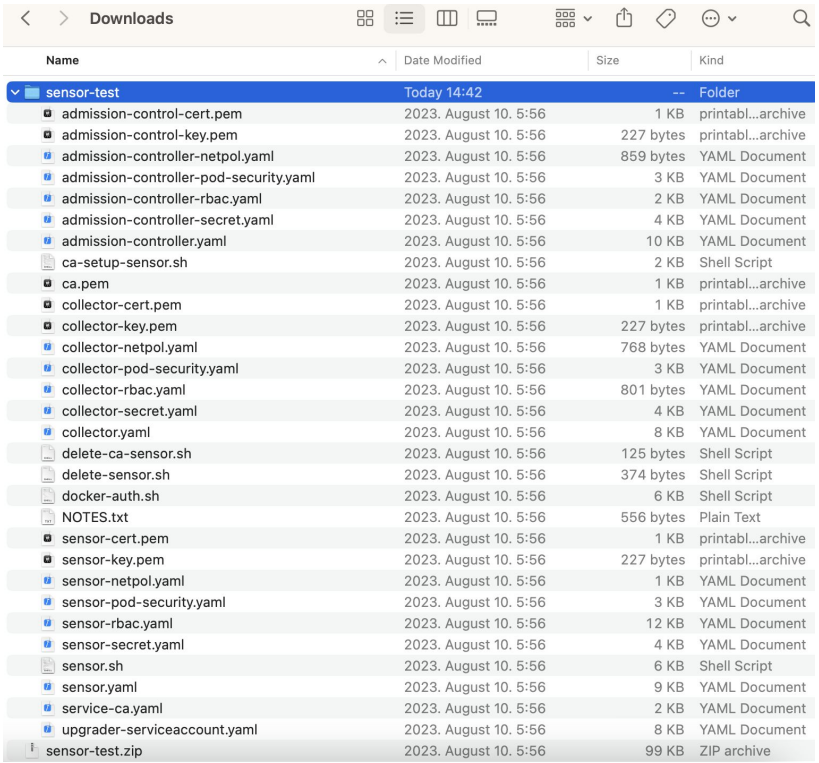
Установка sensor

Скачали bundle



Установка sensor

Распаковали



DevOops

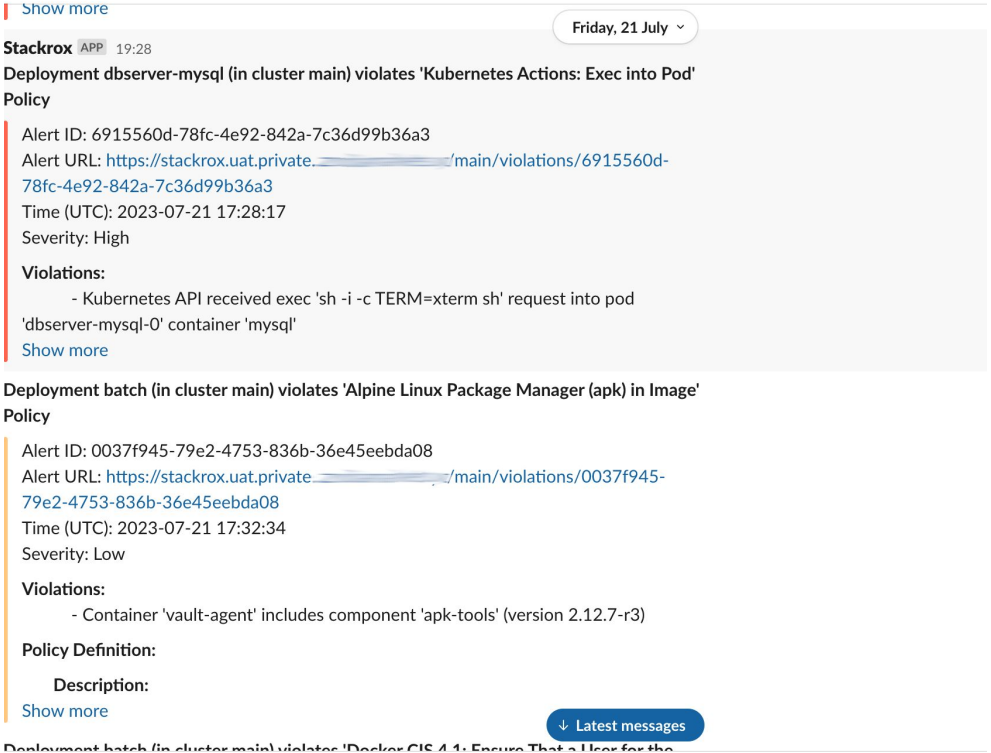
Установка sensor

DevOops

```yaml
---
apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: stackrox-secured-cluster-services
  namespace: stackrox
spec:
  install:
    remediation:
      retries: 3
  upgrade:
    remediation:
      retries: 3
  releaseName: stackrox-secured-cluster-services
  chart:
    spec:
      chart: stackrox-secured-cluster-services
      sourceRef:
        kind: HelmRepository
        name: stackrox
      version: '74.1.0'
  interval: 1m0s
  values:
    helmManaged: true
    clusterName: test # ДОЛЖНО СОВПАДАТЬ с названием кластера в панели
    centralEndpoint: central.stackrox:443
    image:
      main:
        registry: quay.io/stackrox-io
        name: main
        tag: 3.74.1
      collector:
        registry: quay.io/stackrox-io
        name: collector
        tag: 3.74.1
```

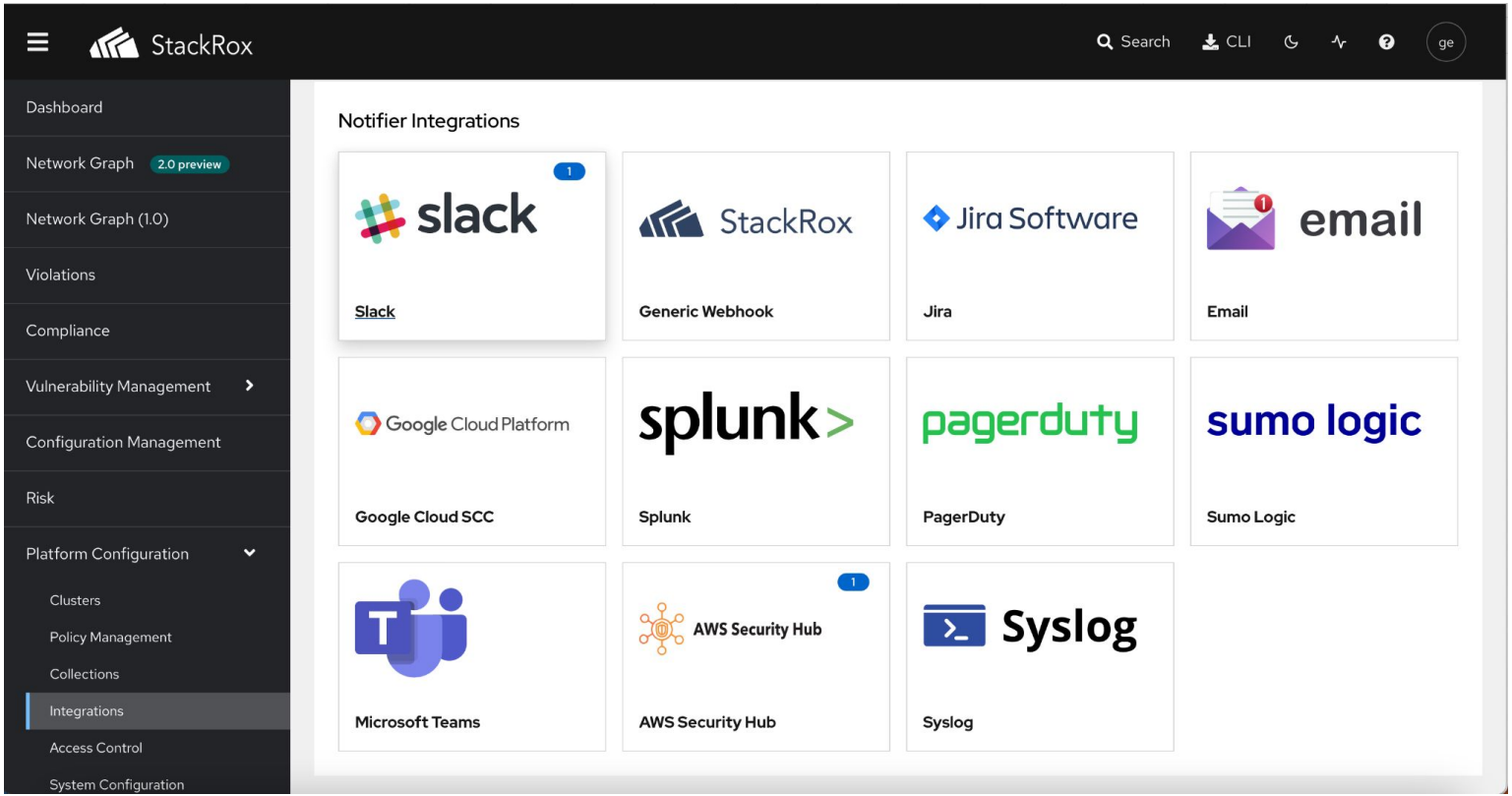
```yaml
admissionControl:
  dynamic:
      disableBypass: false
      enforceOnCreates: false
      enforceOnUpdates: false
      scanInline: false
      timeout: 3
  listenOnCreates: false
  listenOnEvents: true
  listenOnUpdates: false
  serviceTLS:
    cert: |
      # <вставить содержимое файла admission-control-cert.pem>
    key: |
      # <вставить содержимое файла admission-control-key.pem>
ca:
  cert: |
    # <вставить содержимое файла ca.pem>
collector:
  slimMode: false
  collectionMethod: KERNEL_MODULE
  disableTaintTolerations: false
  serviceTLS:
    cert: |
      # <вставить содержимое файла collector-cert.pem>
    key: |
      # <вставить содержимое файла collector-key.pem>
sensor:
  resources:
    requests:
      memory: "1Gi"
      cpu: "0.25"
    limits:
      memory: "4Gi"
      cpu: "2"
  serviceTLS:
    cert: |
      # <вставить содержимое файла sensor-cert.pem>
    key: |
      # <вставить содержимое файла sensor-key.pem>
```

Уведомления в Slack



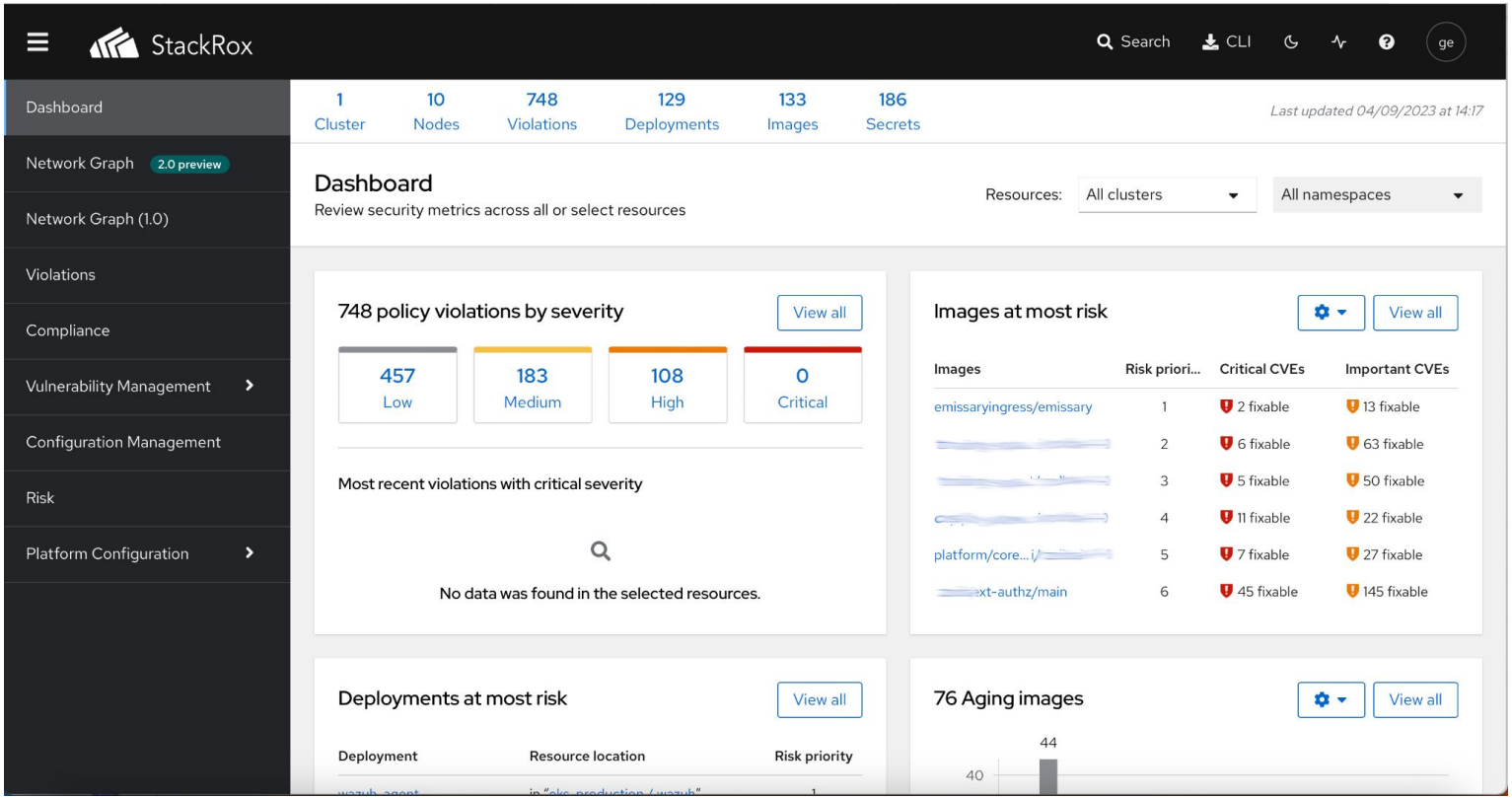
DevOops

Уведомления



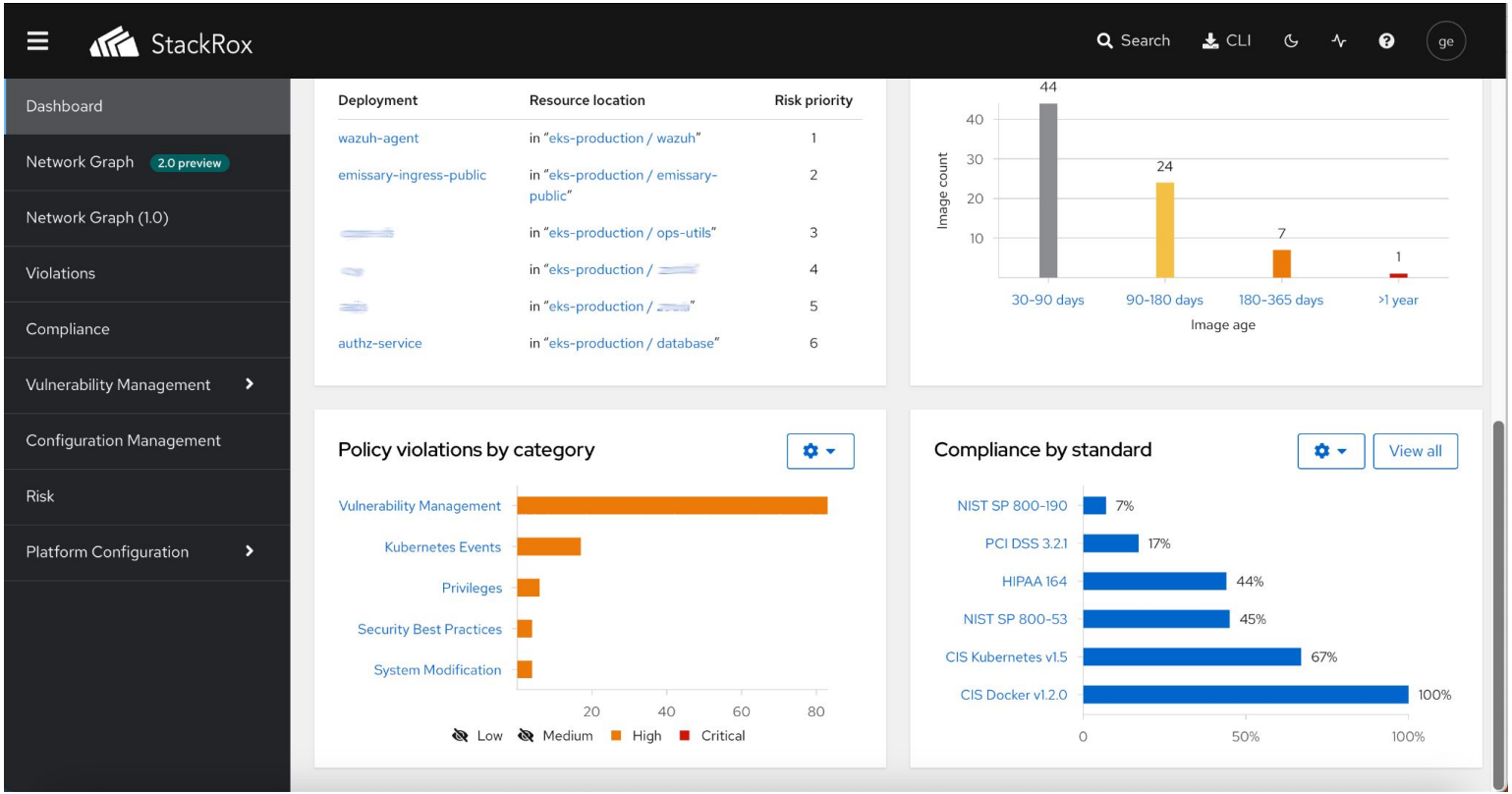
DevOops

Дашборд



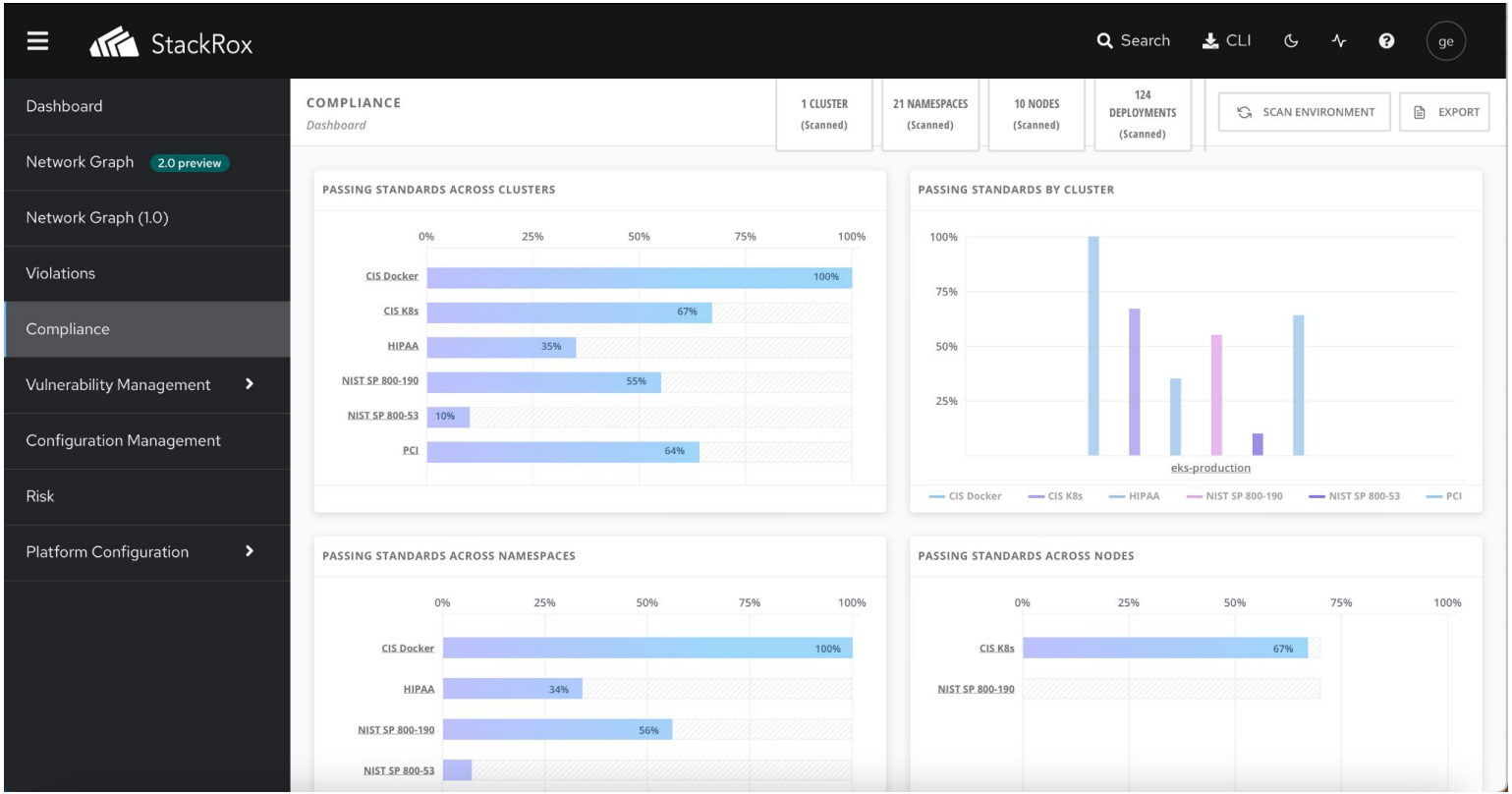
DevOops

Дашборд



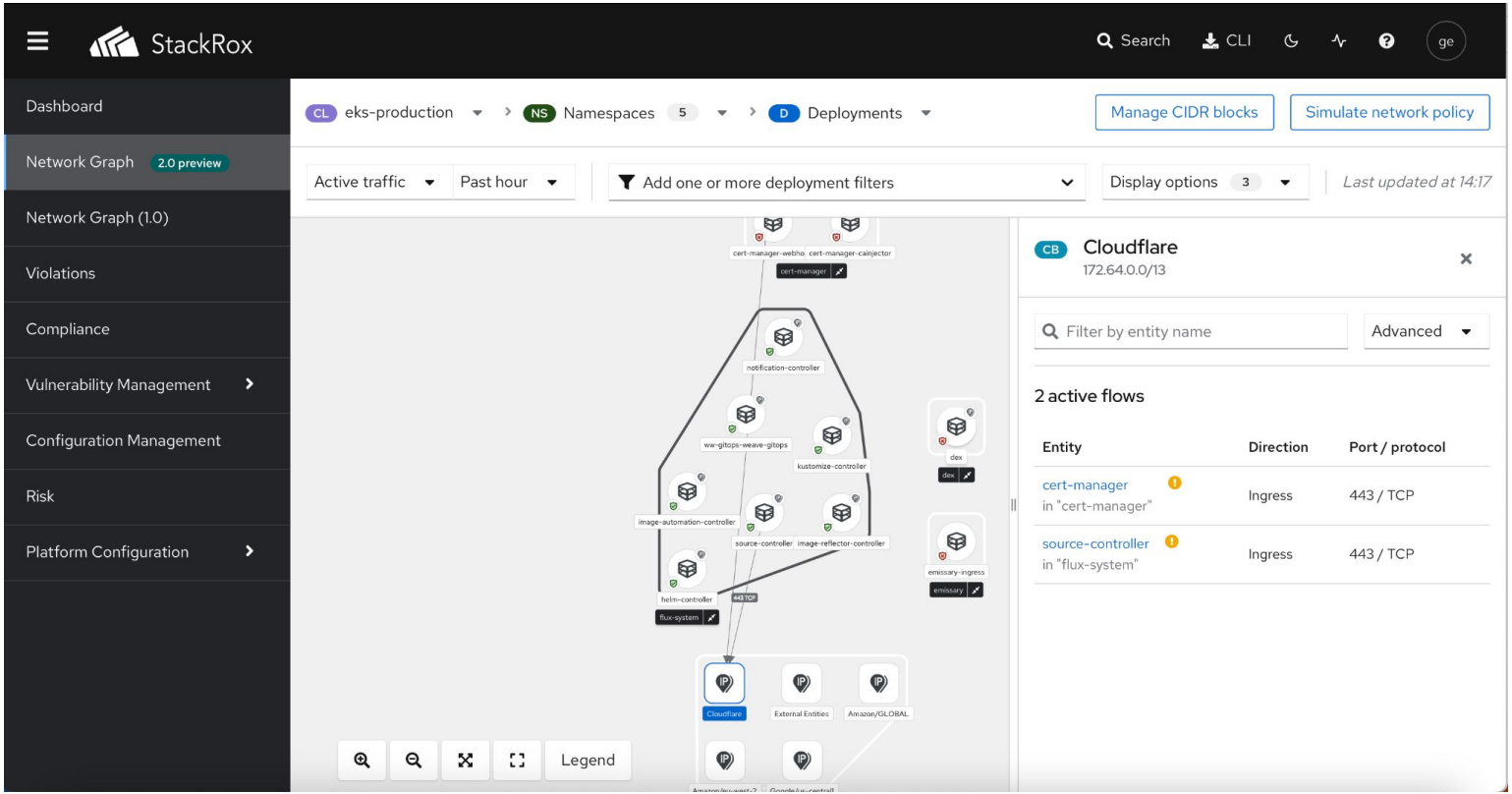
DevOops

Дашборд



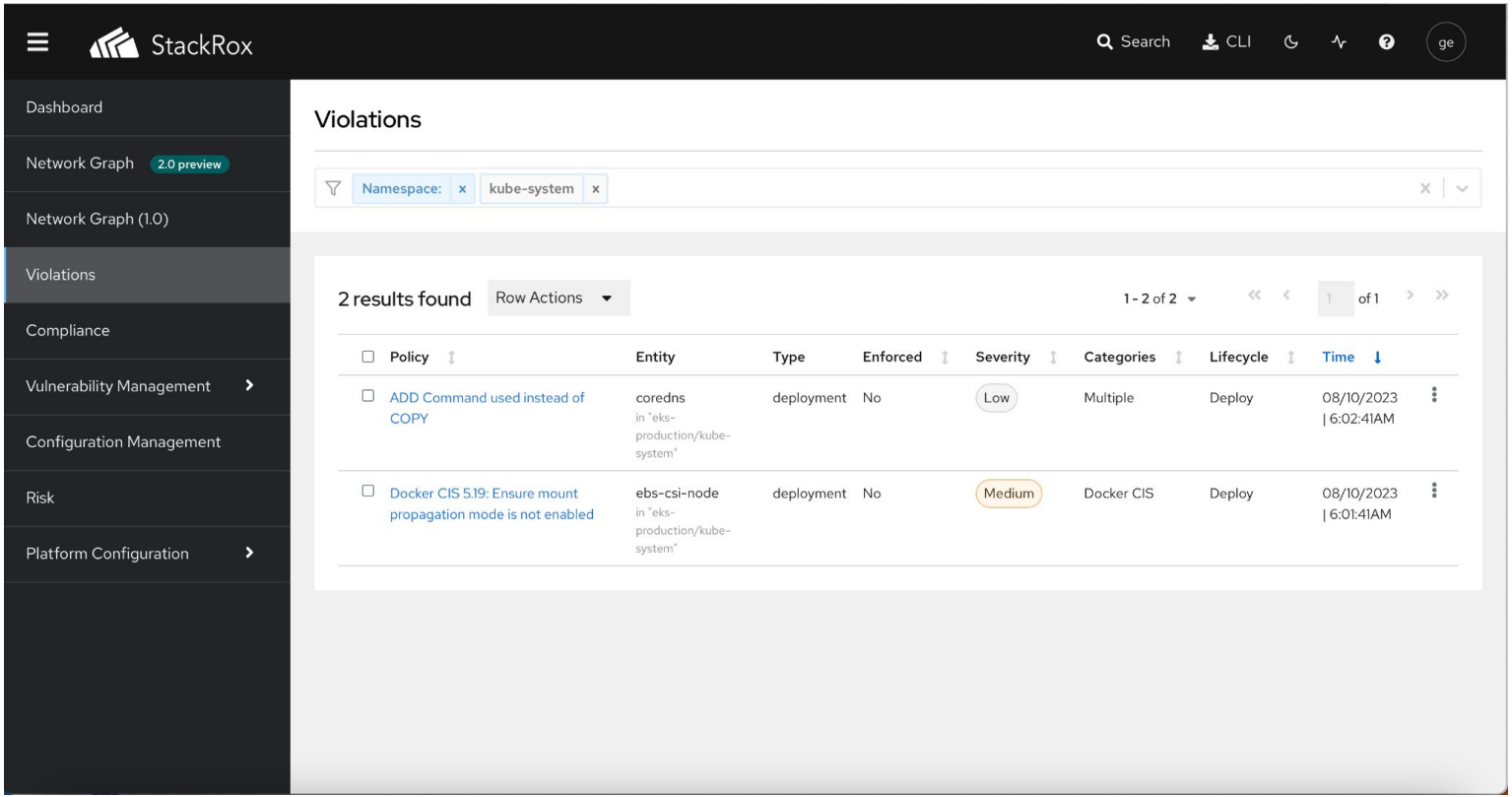
DevOops

Карта сети



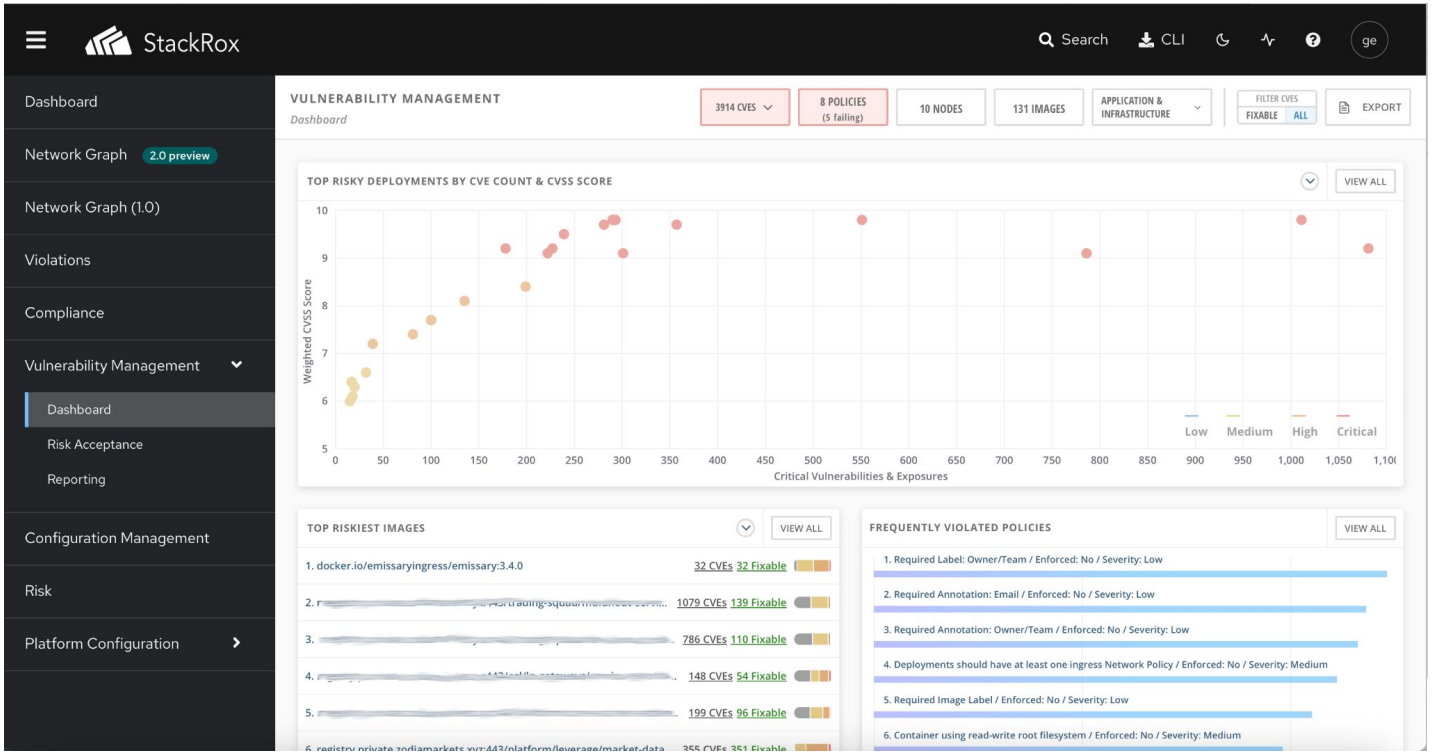
DevOops

Нарушения политик



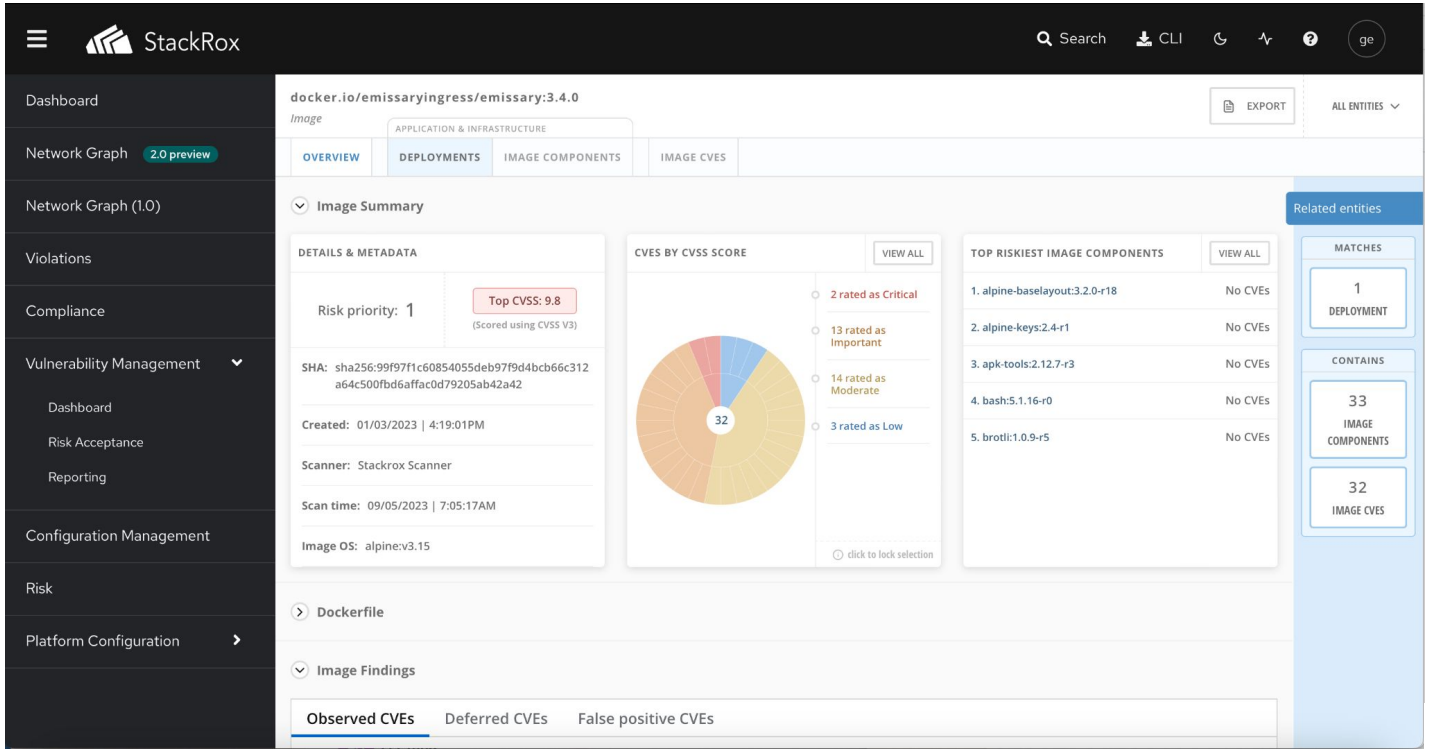
DevOops

Управление уязвимостями - 1



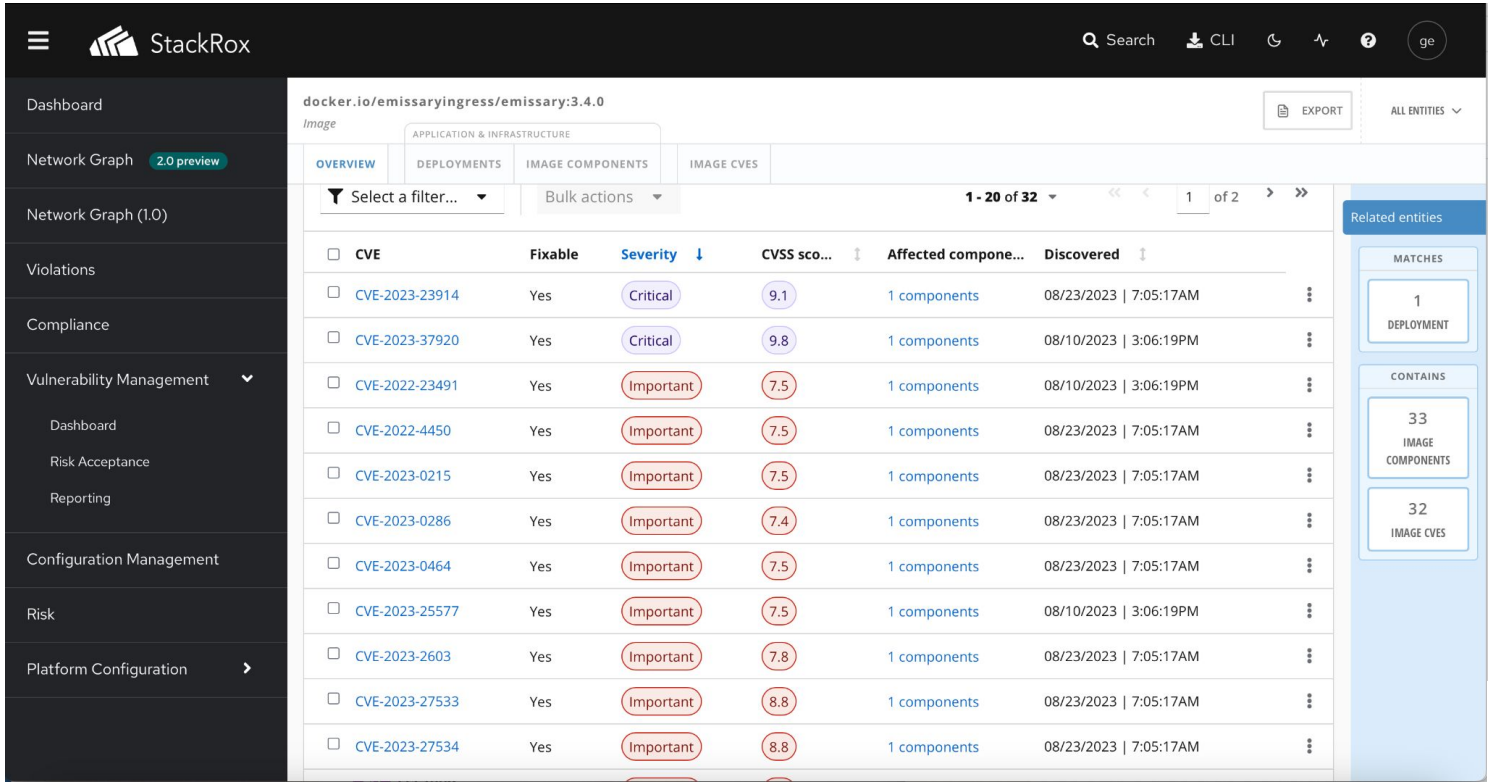
DevOops

Управление уязвимостями - 2



DevOops

Управление уязвимостями - 3

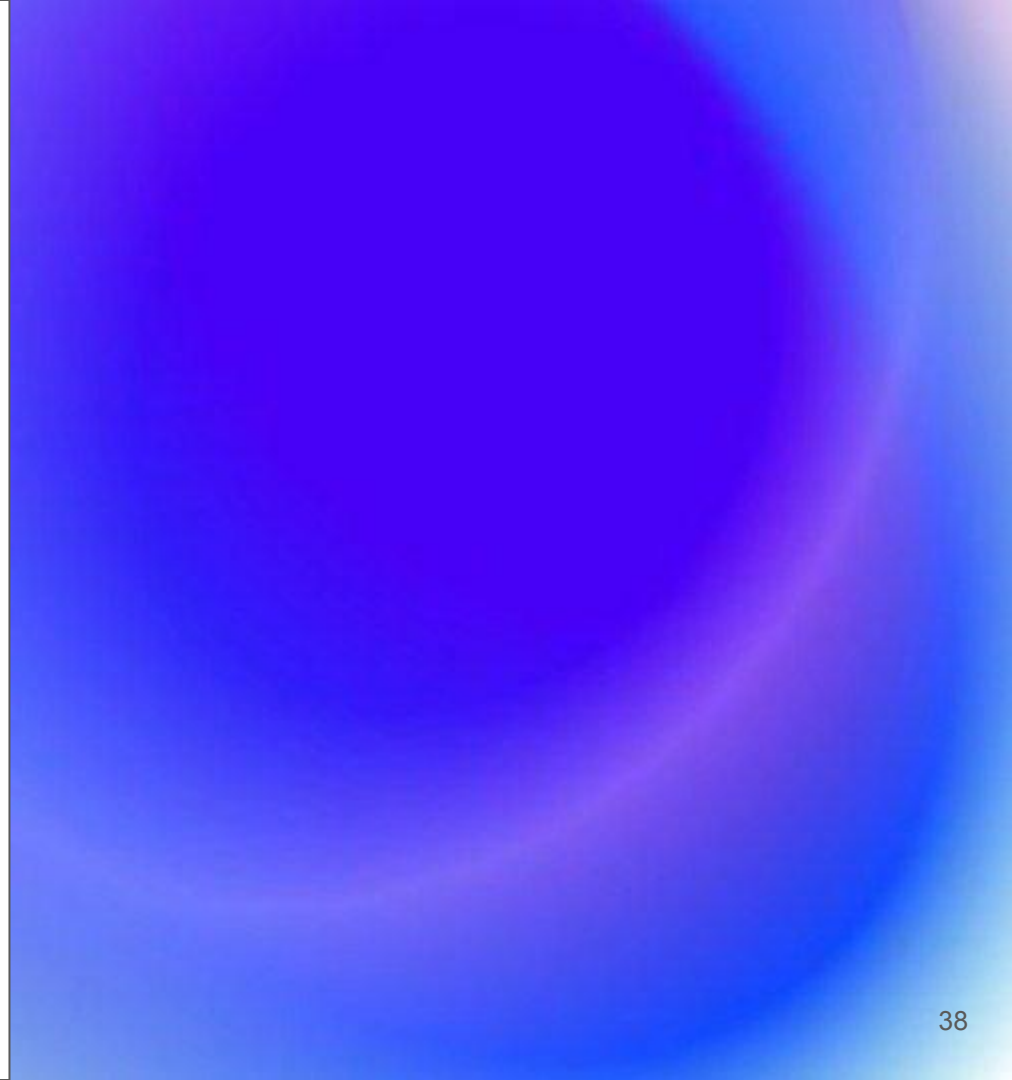


DevOops

Автоматизации?

- terraform provider - https://github.com/splunk/terraform-provider-stackrox (2 года не развивается)
- ansible - НЕТ
- оператор - НЕТ
- зато есть CLI - roxctl: https://docs.openshift.com/acs/4.1/welcome/index.html
  и HTTP(s) API - документации нет, см. исходники

Выводы?



Контакты

https://t.me/gecube

Telegram канал по StackRox:
https://t.me/ru_stackrox

DevOops