
Защищаем Kubernetes при помощи StackRox — дешево, просто, 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 :-)
-

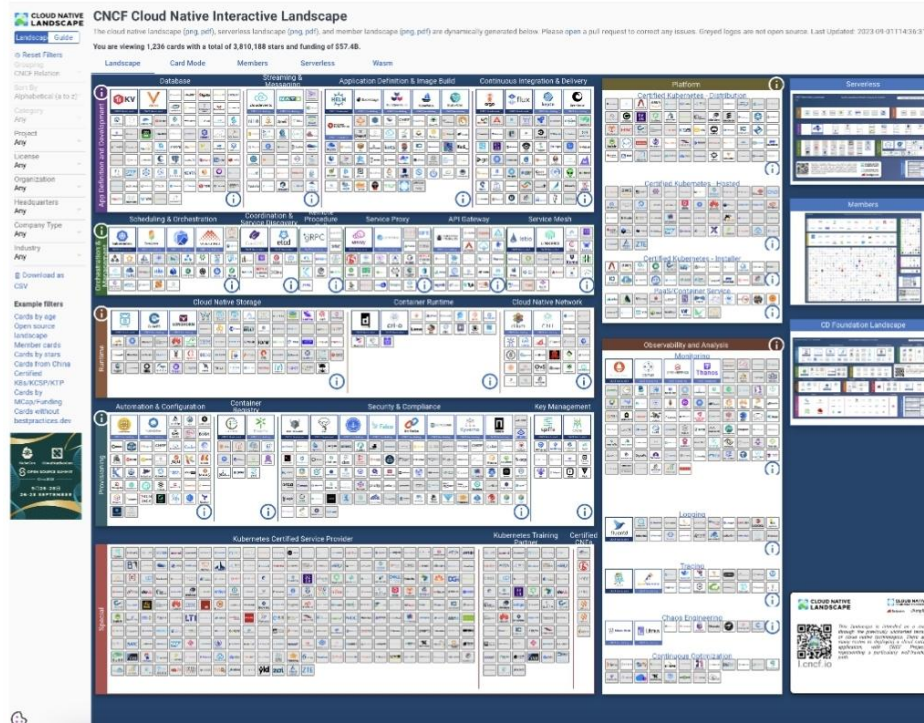
Гипотетическая ситуация



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

































































































Что есть на рынке

<https://landscape.cncf.io>



Что есть на рынке

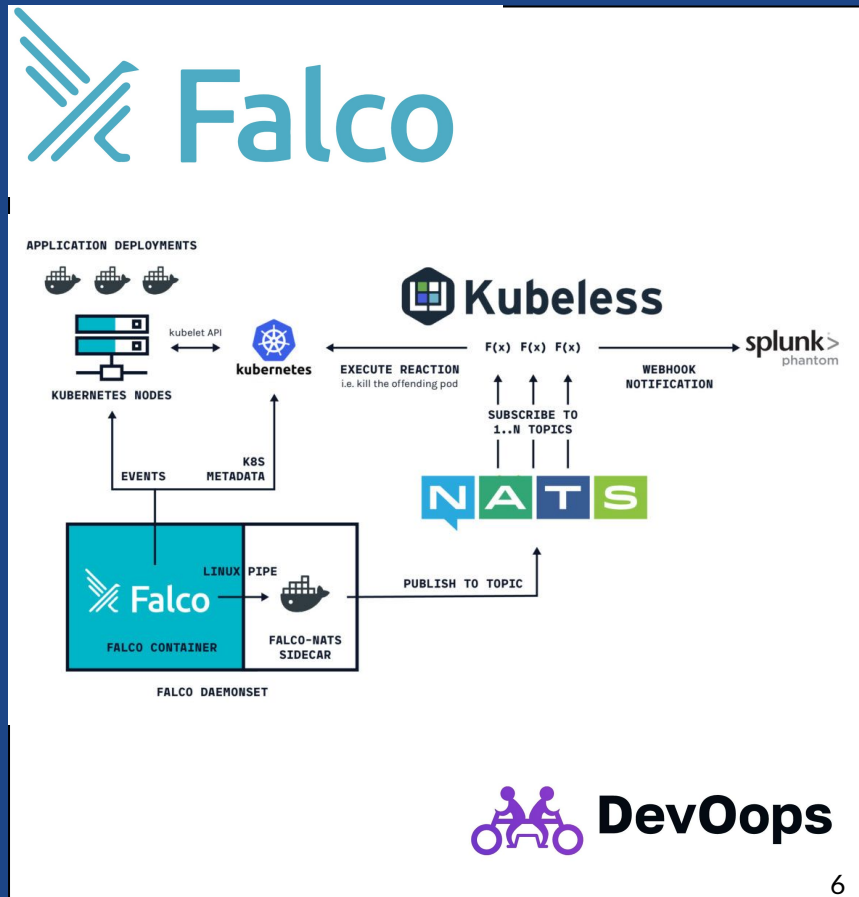
Security & Compliance

 <p>Open Policy Agent</p> <p>CNCF Graduated</p>	 <p>TUF</p> <p>CNCF Graduated</p>	 <p>CERT MANAGER</p> <p>CNCF Incubating</p>	 <p>Falco</p> <p>CNCF Incubating</p>	 <p>in-toto</p> <p>CNCF Incubating</p>	 <p>KEYCLOAK</p> <p>CNCF Incubating</p>	 <p>Kyverno</p> <p>CNCF Incubating</p>	 <p>notary</p> <p>CNCF Incubating</p>	 <p>AIRLOCK</p>								
 <p>anchore</p>	 <p>API Clarity</p>	 <p>apolicy</p>	 <p>aqua</p>	 <p>ARMO</p>	 <p>Aserto</p>	 <p>BLACKDUCK</p>	 <p>BLOOMBASE</p>	 <p>CAPSULE8</p>	 <p>cerbos</p>	 <p>Check Point</p>	 <p>checkov</p>	 <p>CHEF INSPEC</p>	 <p>clair</p>	 <p>CLOUDMATS</p>	 <p>CONFIDENTIAL CONTAINERS</p>	
 <p>ContainersSSH</p>	 <p>Curiefense</p>	 <p>Datica</p>	 <p>datree</p>	 <p>dex</p>	 <p>DOSEC 小盾科技</p>	 <p>EJBCA</p>	 <p>Fairwinds Insights</p>	 <p>FOSSA</p>	 <p>FOSSID</p>	 <p>Fugue</p>	 <p>Goldilocks</p>	 <p>Grafeas</p>	 <p>Hexa</p>	 <p>Keylime</p>	 <p>KICS</p>	
 <p>KSOC</p>	 <p>kube-bench</p>	 <p>kube-hunter</p>	 <p>kubearmor</p>	 <p>KUBE Clarity</p>	 <p>KubeLinter</p>	 <p>Kubescape</p>	 <p>KUBEWARDEN</p>	 <p>matano</p>	 <p>Metarget</p>	 <p>mondoo</p>	 <p>MoranSec</p>	 <p>NeuVector</p>	 <p>nirmata</p>	 <p>opcr</p>	 <p>OpenFGA</p>	 <p>OpenSCAP</p>
 <p>orca security</p>	 <p>Oxeye</p>	 <p>PALADIN CLOUD</p>	 <p>PARALUS</p>	 <p>PARSEC</p>	 <p>Passage</p>	 <p>pluto</p>	 <p>polaris</p>	 <p>portshift</p>	 <p>PRISMA CLOUD</p>	 <p>青藤云安全</p>	 <p>RBAC LOOKUP</p>	 <p>rbac manager</p>	 <p>Rudder</p>	 <p>scribe</p>	 <p>sigstore</p>	 <p>Slim</p>
 <p>snyk</p>	 <p>nexus repository</p>	 <p>SONBUOY</p>	 <p>SOPS</p>	 <p>SPYDERBAT</p>	 <p>STACKHAWK</p>	 <p>StackRox</p>	 <p>sysdig SECURE</p>	 <p>探真科技</p>	 <p>terrascan</p>	 <p>Tetragon</p>	 <p>ThreatMapper</p>	 <p>TIGERA</p>	 <p>TOPAZ</p>	 <p>TREND MICRO</p>	 <p>trivy</p>	 <p>trivy</p>
 <p>VEINMIND</p>	 <p>VM Clarity</p>	 <p>WhiteSource</p>	 <p>Zettaset</p>													



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
- CM.
- <https://github.com/draios/sysdig> и <https://github.com/draios/sysdig-in-spect>

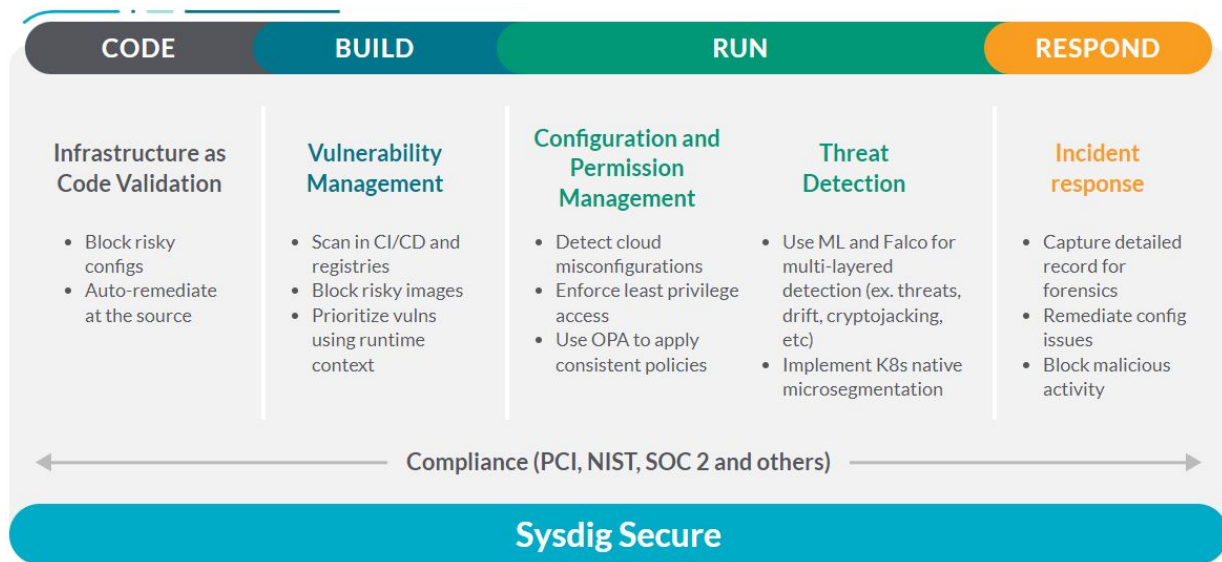


Что есть на рынке



На базе falco сделан платный
SysDig Secure

<https://sysdig.com/>



Что есть на рынке



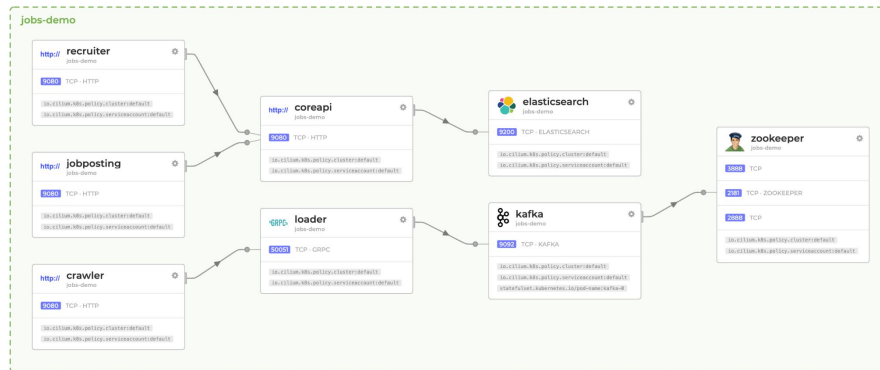
Tetragon

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

зато с Cilium у нас есть Hubble!



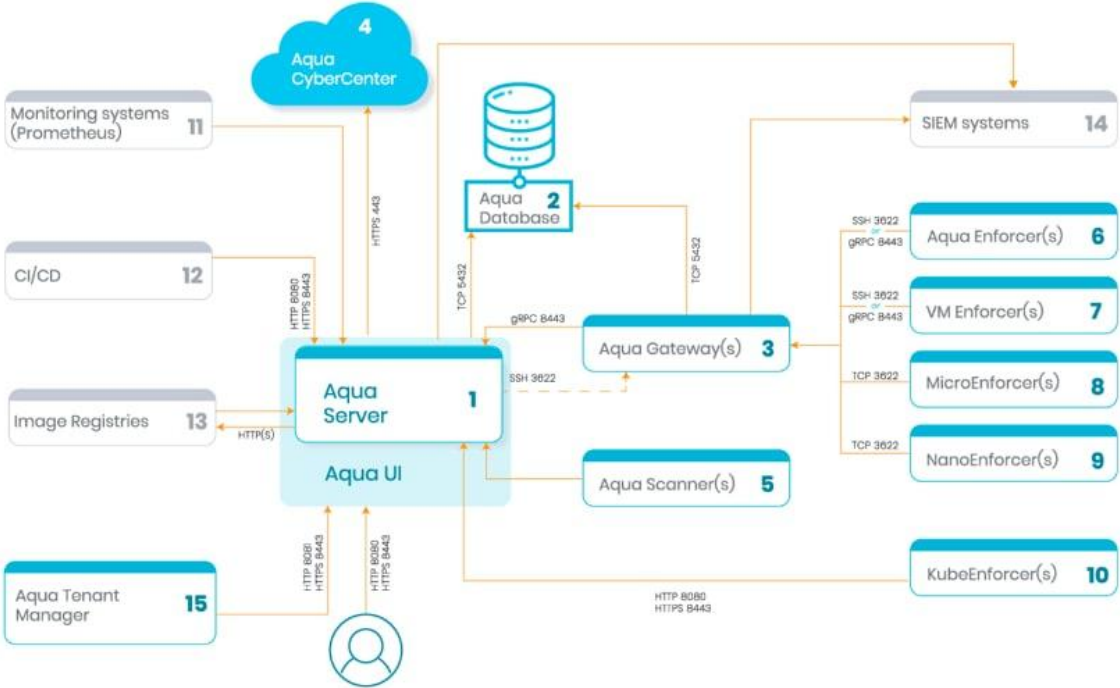
Hubble



Что есть на рынке



Aqua Security



Что есть на рынке



kube-bench

aqua
kube-bench

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



kube-hunter

aqua
kube-hunter

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



DevOops

Что есть на рынке

куча различных сканеров образов



<https://github.com/quay/clair>



aqua
trivy

<https://github.com/aquasecurity/trivy>

anchore

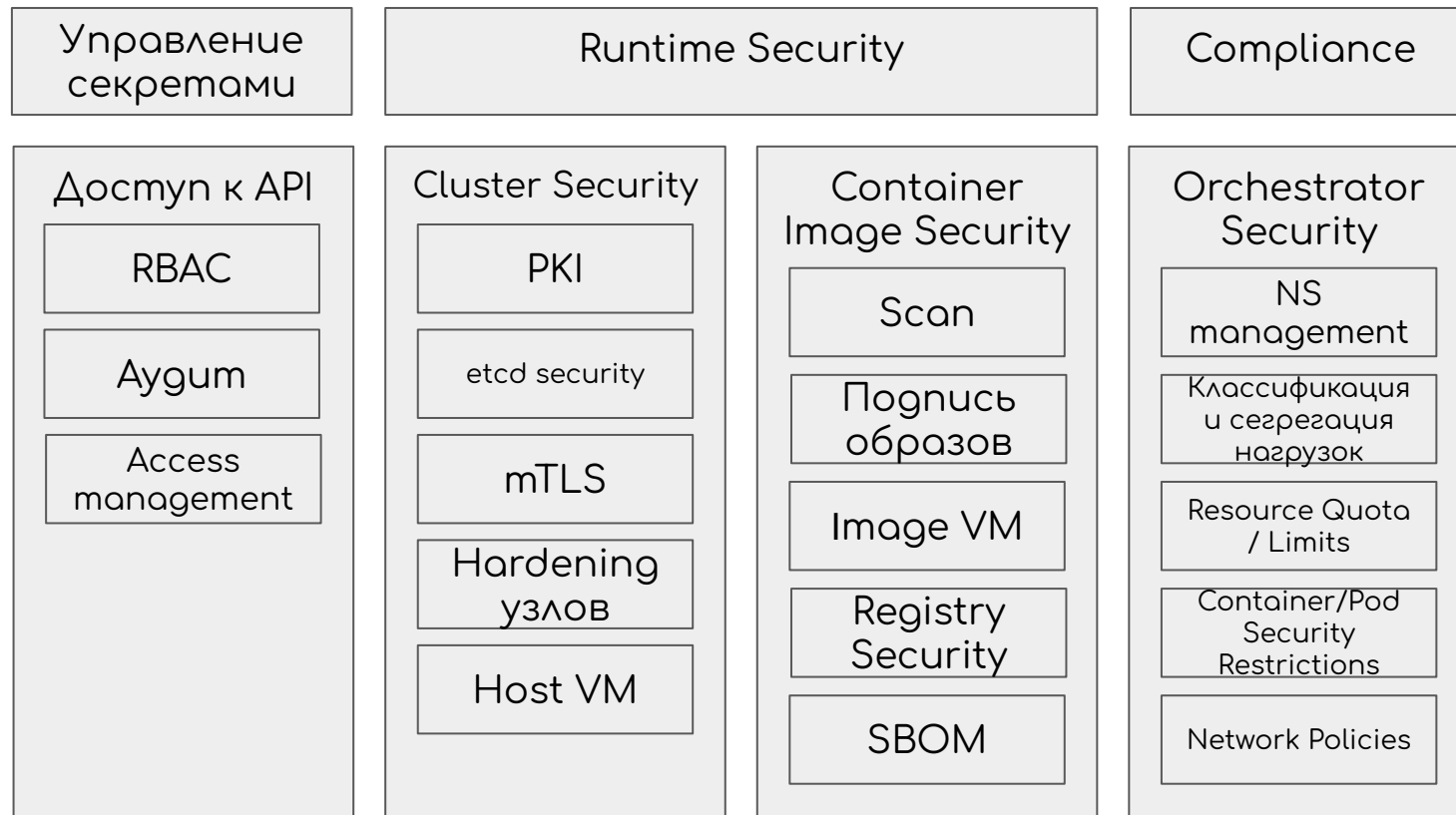
<https://github.com/anchore/anchore-engine>

(deprecated)

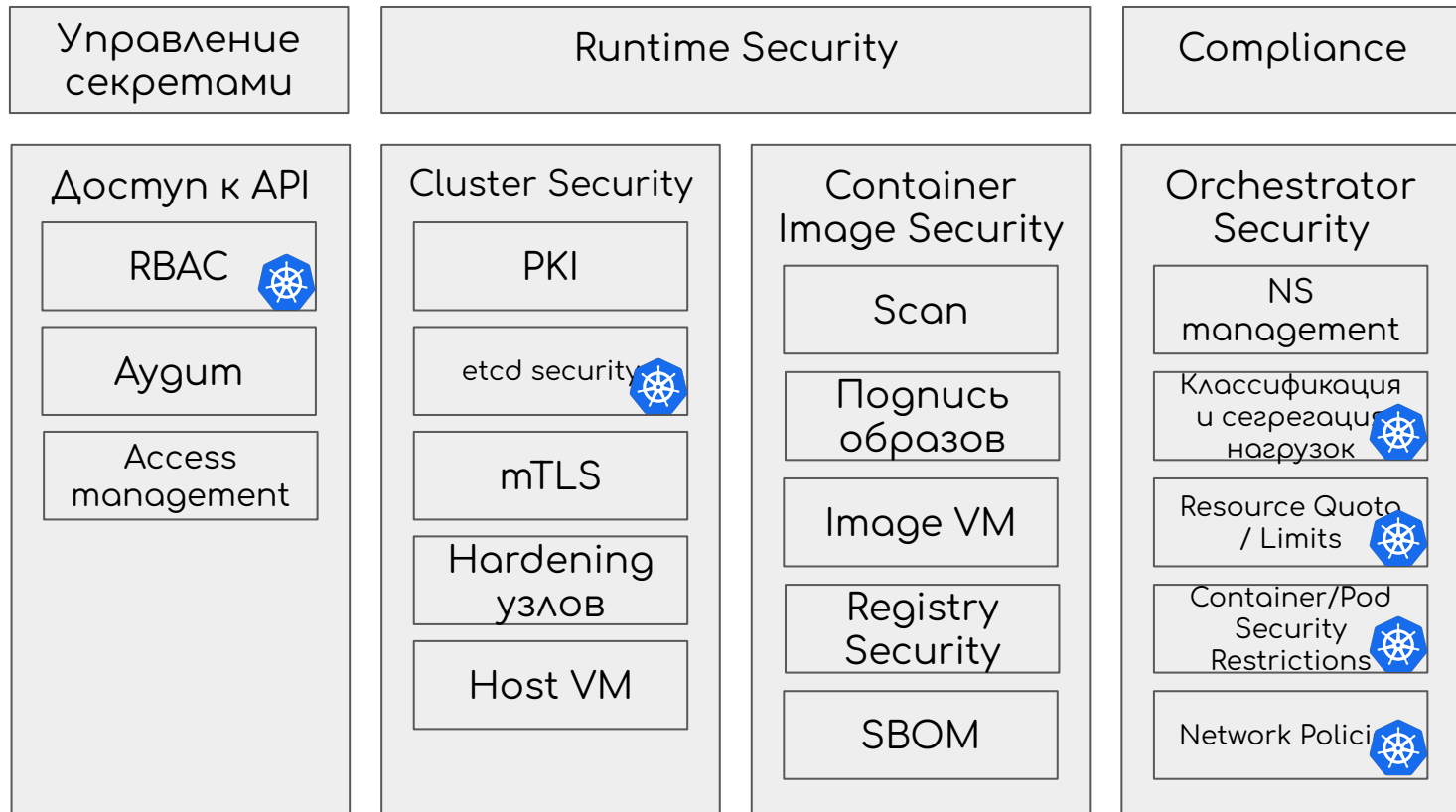


DevOps

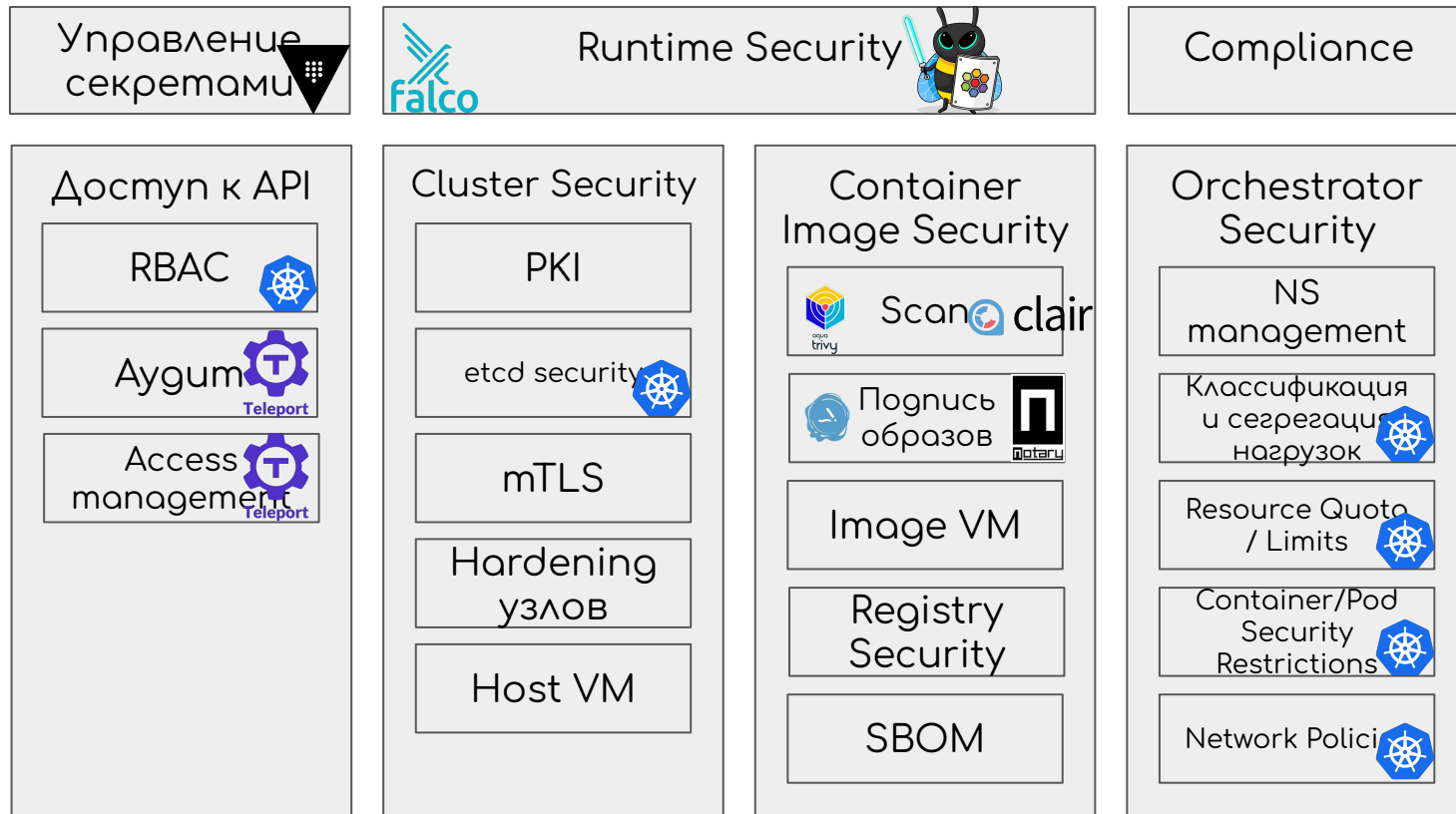
Безопасность kubernetes



Безопасность kubernetes

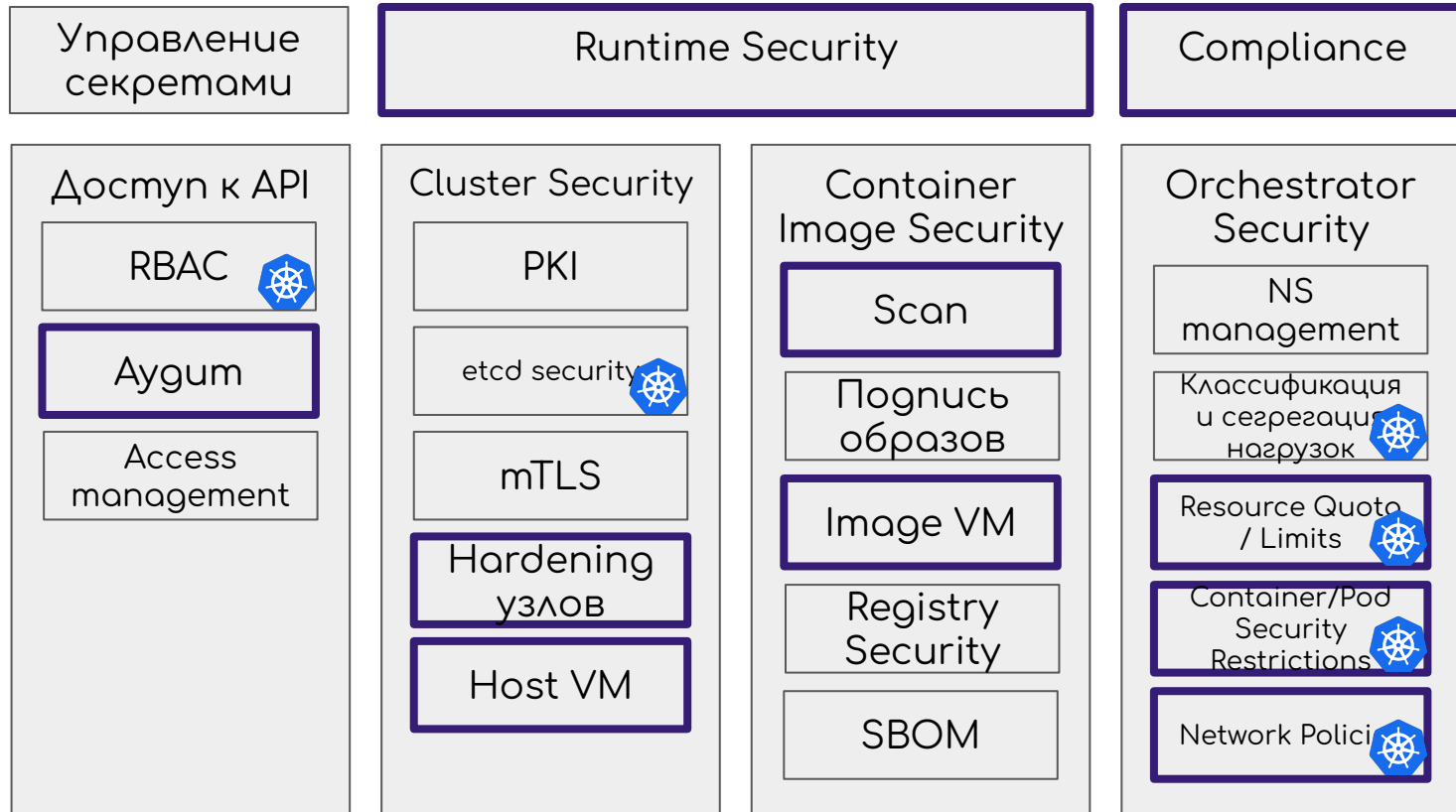


Безопасность kubernetes

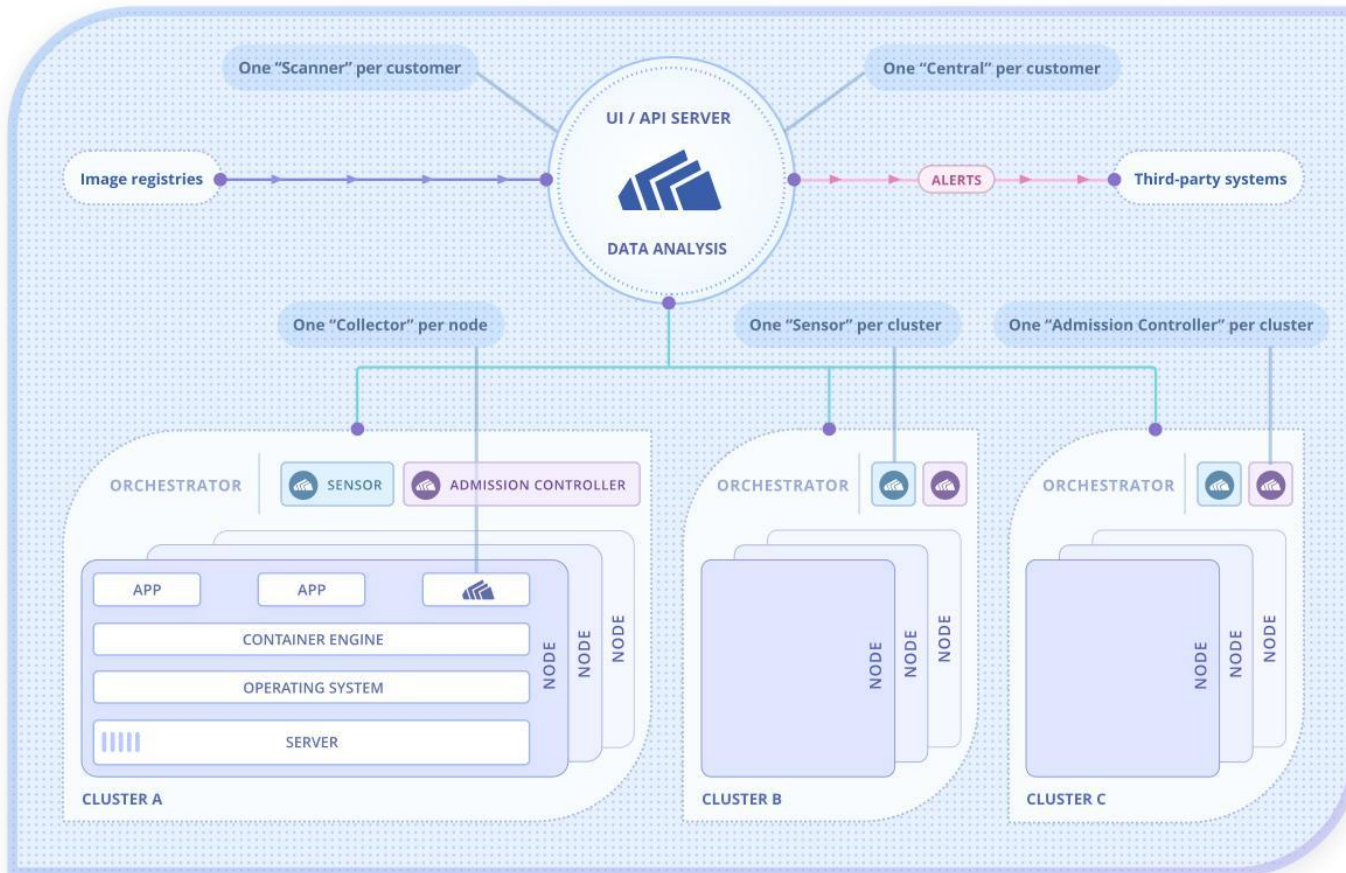


Безопасность kubernetes

StackRox



Архитектура StackRox



Установка

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

Установка central

```
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
```

```
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
    httpassword: |
      admin:$2y$05$Ssd5ZuAD3bCX9ddhokQhS.2zLRisC2ZeLFXi/meQ.WZi5ykxrLZRm
      georg:$2y$05$WnbMo0H0aZLZJaQ9bHd3TOirRpw/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: QxY4bVYPHgTzBYL04Nb28ywS8 # 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

The screenshot displays the StackRox interface. On the left is a dark sidebar with a menu containing: Dashboard, Network Graph (2.0 preview), Network Graph (1.0), Violations, Compliance, Vulnerability Management, Configuration Management, Risk, Platform Configuration (with a dropdown arrow), Clusters (highlighted), Policy Management, Collections, Integrations, Access Control, and System Configuration. The main content area has a top navigation bar with a search icon, 'Search', 'CLI', a refresh icon, a home icon, a help icon, and a user profile 'ge'. Below this is a 'CLUSTERS Resource List' section with a filter input 'Add one or more filters' and a 'MANAGE TOKENS' button. A toggle for 'Automatically upgrade secured clusters' is turned on. There are buttons for 'UPGRADE (0)', 'DELETE (0)', and 'Install cluster'. A table lists one cluster:

<input type="checkbox"/>	Name	Cloud Provider	Cluster Status	Sensor Upgrade	Credential Expiration	Cluster Deletion
<input type="checkbox"/>	eks-production	AWS eu-west-2	Healthy Collector Sensor AdmissionControl	Up to date with Central	in 11 months	Not applicable




Установка sensor

Заходим в список кластеров и выбираем “New Cluster”

CLUSTERS
Resource List

1 CLUSTER

 Automatically upgrade secured clusters
UPGRADE (0)
DELETE (0)

<input type="checkbox"/>	Name	Cloud Provider	Cluster Status	Sensor Upgrade	Credential Expiration
<input type="checkbox"/>	eks-production 	AWS eu-west-2	✔ Healthy ✔ Collector ✔ Sensor ✔ AdmissionControl 	✔ Up to date with Central	✔ in 11 months

Установка sensor

Выбираем опции

Test → NEXT ×

Static Configuration (requires deployment)

Cluster Name (required)

Cluster Type (required)

Main Image Repository (required)

Central API Endpoint (include port) (required)

Collection Method

Collector Image Repository (uses Main image repository by default)

Dynamic Configuration (syncs with Sensor)

Custom default image registry
Set a value if the default registry is not docker.io in this cluster

Enforce on Object Creates

Enforce on Object Updates

Timeout (seconds)

Contact Image Scanners

Disable Use of Bypass Annotation

Enable Cluster Audit Logging

This setting will not work for Kubernetes or OpenShift 3.x. To enable logging, you must upgrade your cluster to OpenShift 4 or higher.

Установка sensor


Скачиваем bundle

Test ✓ FINISH ×

1. Download files

Download the required configuration files, keys, and scripts.

Configure cluster to allow future automatic upgrades

[DOWNLOAD YAML FILE AND KEYS](#) 

Modify the YAML files to suit your environment if needed.
Do not reuse this bundle for more than one cluster.

2. Deploy

Use the deploy script inside the bundle to set up your cluster.

Waiting for the cluster to check in successfully...

Download helm values

To start managing this cluster with a Helm chart, you can download the cluster's current configuration values in Helm format.

[DOWNLOAD HELM VALUES](#)


Установка sensor

Кластер переходит в “not applicable” состояние

CLUSTERS MANAGE TOKENS

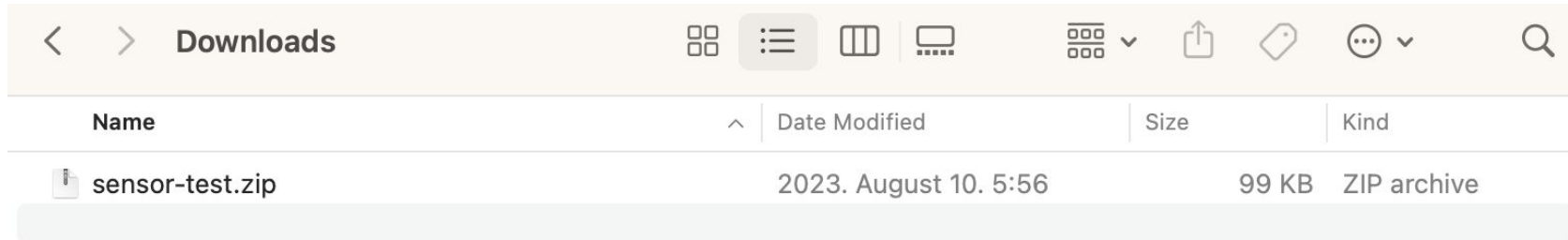
Resource List

2 CLUSTERS Automatically upgrade secured clusters UPGRADE (0) DELETE (0) Install cluster


<input type="checkbox"/>	Name	Cloud Provider	Cluster Status	Sensor Upgrade	Credential Expiration	Cluster Deletion
<input type="checkbox"/>	eks-production 	AWS eu-west-2	✓ Healthy ✓ Collector ✓ Sensor ✓ AdmissionControl	✓ Up to date with Central	✓ in 11 months	Not applicable
<input type="checkbox"/>	test	Not applicable	⊘ Uninitialized ⊘ Collector ⊘ Sensor ⊘ AdmissionControl	Not applicable	Not applicable	Not applicable

Установка sensor

Скачали bundle

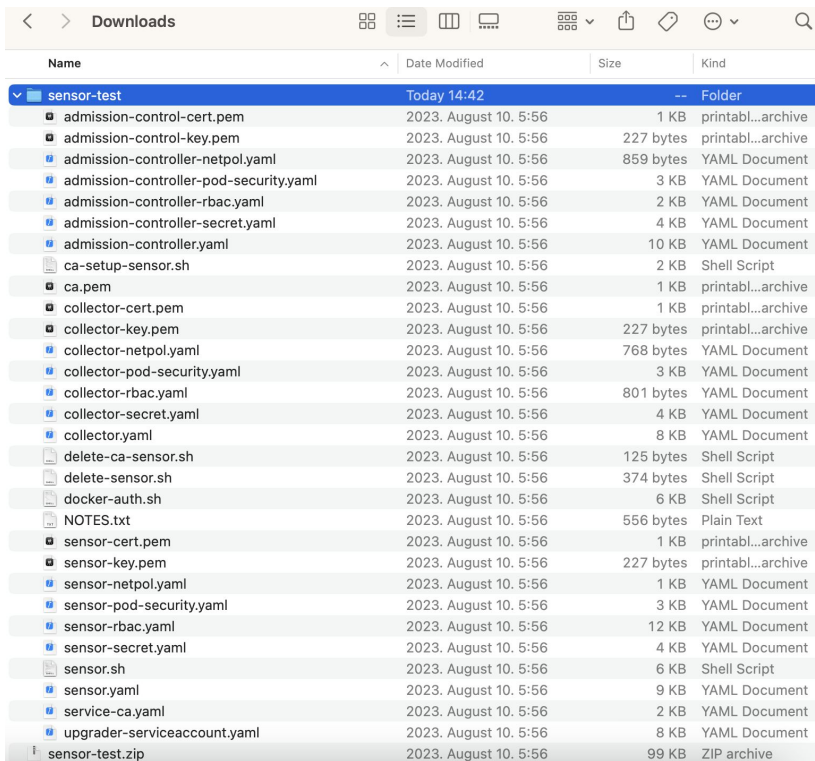


The screenshot shows a file manager interface for the 'Downloads' folder. The interface includes navigation arrows, the folder name 'Downloads', and several icons for view and actions. Below the navigation bar is a table with columns for Name, Date Modified, Size, and Kind. A single file, 'sensor-test.zip', is listed with a date of '2023. August 10. 5:56', a size of '99 KB', and a kind of 'ZIP archive'.

Name	Date Modified	Size	Kind
 sensor-test.zip	2023. August 10. 5:56	99 KB	ZIP archive

Установка sensor

Распаковали



Name	Date Modified	Size	Kind
sensor-test	Today 14:42	--	Folder
admission-control-cert.pem	2023. August 10. 5:56	1 KB	printabl...archive
admission-control-key.pem	2023. August 10. 5:56	227 bytes	printabl...archive
admission-controller-netpol.yaml	2023. August 10. 5:56	859 bytes	YAML Document
admission-controller-pod-security.yaml	2023. August 10. 5:56	3 KB	YAML Document
admission-controller-rbac.yaml	2023. August 10. 5:56	2 KB	YAML Document
admission-controller-secret.yaml	2023. August 10. 5:56	4 KB	YAML Document
admission-controller.yaml	2023. August 10. 5:56	10 KB	YAML Document
ca-setup-sensor.sh	2023. August 10. 5:56	2 KB	Shell Script
ca.pem	2023. August 10. 5:56	1 KB	printabl...archive
collector-cert.pem	2023. August 10. 5:56	1 KB	printabl...archive
collector-key.pem	2023. August 10. 5:56	227 bytes	printabl...archive
collector-netpol.yaml	2023. August 10. 5:56	768 bytes	YAML Document
collector-pod-security.yaml	2023. August 10. 5:56	3 KB	YAML Document
collector-rbac.yaml	2023. August 10. 5:56	801 bytes	YAML Document
collector-secret.yaml	2023. August 10. 5:56	4 KB	YAML Document
collector.yaml	2023. August 10. 5:56	8 KB	YAML Document
delete-ca-sensor.sh	2023. August 10. 5:56	125 bytes	Shell Script
delete-sensor.sh	2023. August 10. 5:56	374 bytes	Shell Script
docker-auth.sh	2023. August 10. 5:56	6 KB	Shell Script
NOTES.txt	2023. August 10. 5:56	556 bytes	Plain Text
sensor-cert.pem	2023. August 10. 5:56	1 KB	printabl...archive
sensor-key.pem	2023. August 10. 5:56	227 bytes	printabl...archive
sensor-netpol.yaml	2023. August 10. 5:56	1 KB	YAML Document
sensor-pod-security.yaml	2023. August 10. 5:56	3 KB	YAML Document
sensor-rbac.yaml	2023. August 10. 5:56	12 KB	YAML Document
sensor-secret.yaml	2023. August 10. 5:56	4 KB	YAML Document
sensor.sh	2023. August 10. 5:56	6 KB	Shell Script
sensor.yaml	2023. August 10. 5:56	9 KB	YAML Document
service-ca.yaml	2023. August 10. 5:56	2 KB	YAML Document
upgrader-serviceaccount.yaml	2023. August 10. 5:56	8 KB	YAML Document
sensor-test.zip	2023. August 10. 5:56	99 KB	ZIP archive

Установка sensor

```
---
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
```

```
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: "16Gi"
        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

[Show more](#)

Friday, 21 July

Stackrox APP 19:28

Deployment dbserver-mysql (in cluster main) violates 'Kubernetes Actions: Exec into Pod' Policy

Alert ID: 6915560d-78fc-4e92-842a-7c36d99b36a3
Alert URL: https://stackrox.uat.private._____/main/violations/6915560d-78fc-4e92-842a-7c36d99b36a3
Time (UTC): 2023-07-21 17:28:17
Severity: High

Violations:

- Kubernetes API received exec 'sh -i -c TERM=xterm sh' request into pod 'dbserver-mysql-0' container 'mysql'

[Show more](#)

Deployment batch (in cluster main) violates 'Alpine Linux Package Manager (apk) in Image' Policy

Alert ID: 0037f945-79e2-4753-836b-36e45eebda08
Alert URL: https://stackrox.uat.private._____/main/violations/0037f945-79e2-4753-836b-36e45eebda08
Time (UTC): 2023-07-21 17:32:34
Severity: Low

Violations:

- Container 'vault-agent' includes component 'apk-tools' (version 2.12.7-r3)

Policy Definition:

Description:

[Show more](#)

[↓ Latest messages](#)

Deployment batch (in cluster main) violates 'Docker CIS 4.1: Ensure That a User for the

Уведомления

StackRox

Search CLI

Dashboard

Network Graph **2.0 preview**

Network Graph (1.0)

Violations

Compliance

Vulnerability Management

Configuration Management

Risk

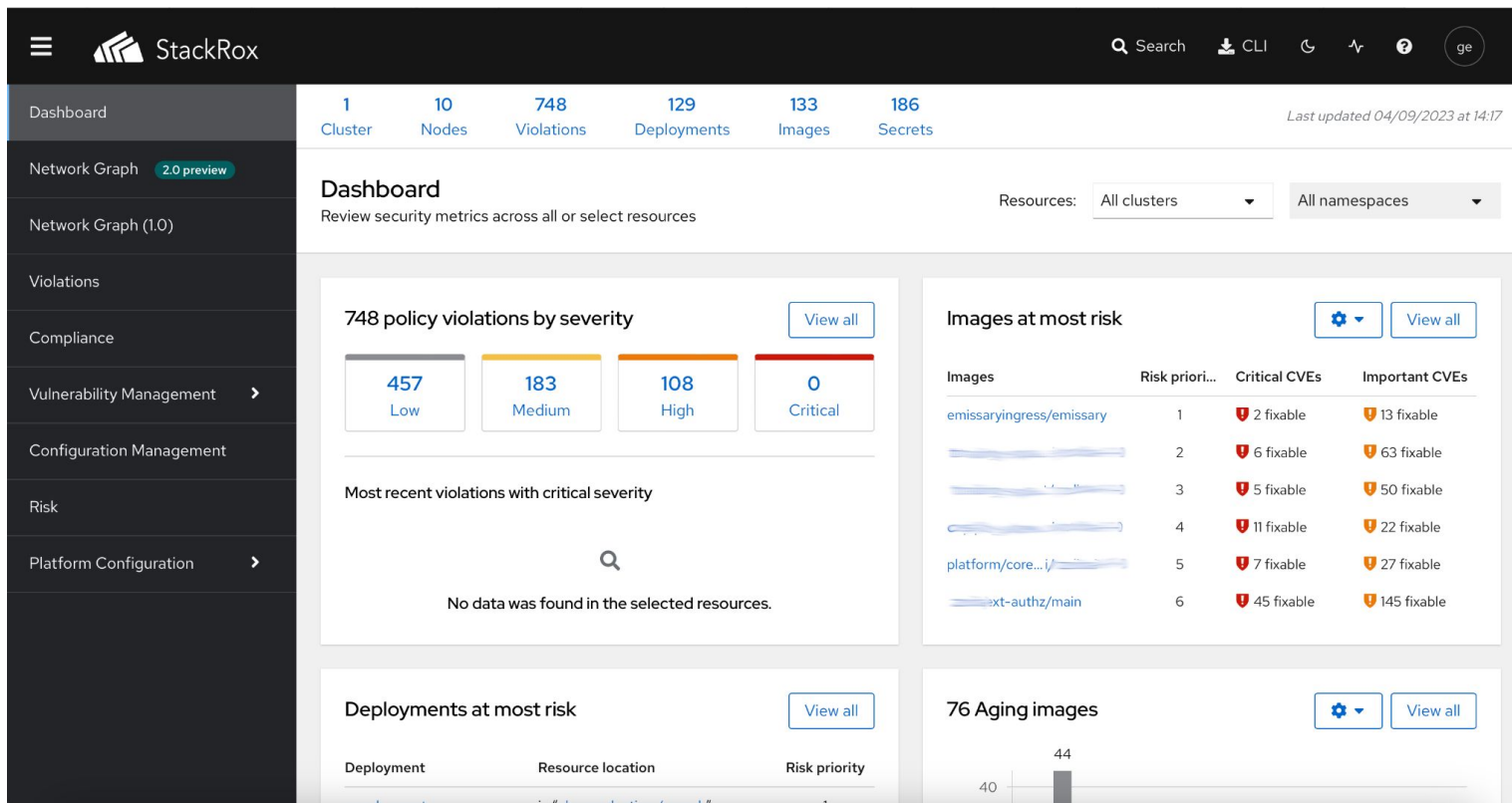
Platform Configuration

- Clusters
- Policy Management
- Collections
- Integrations**
- Access Control
- System Configuration

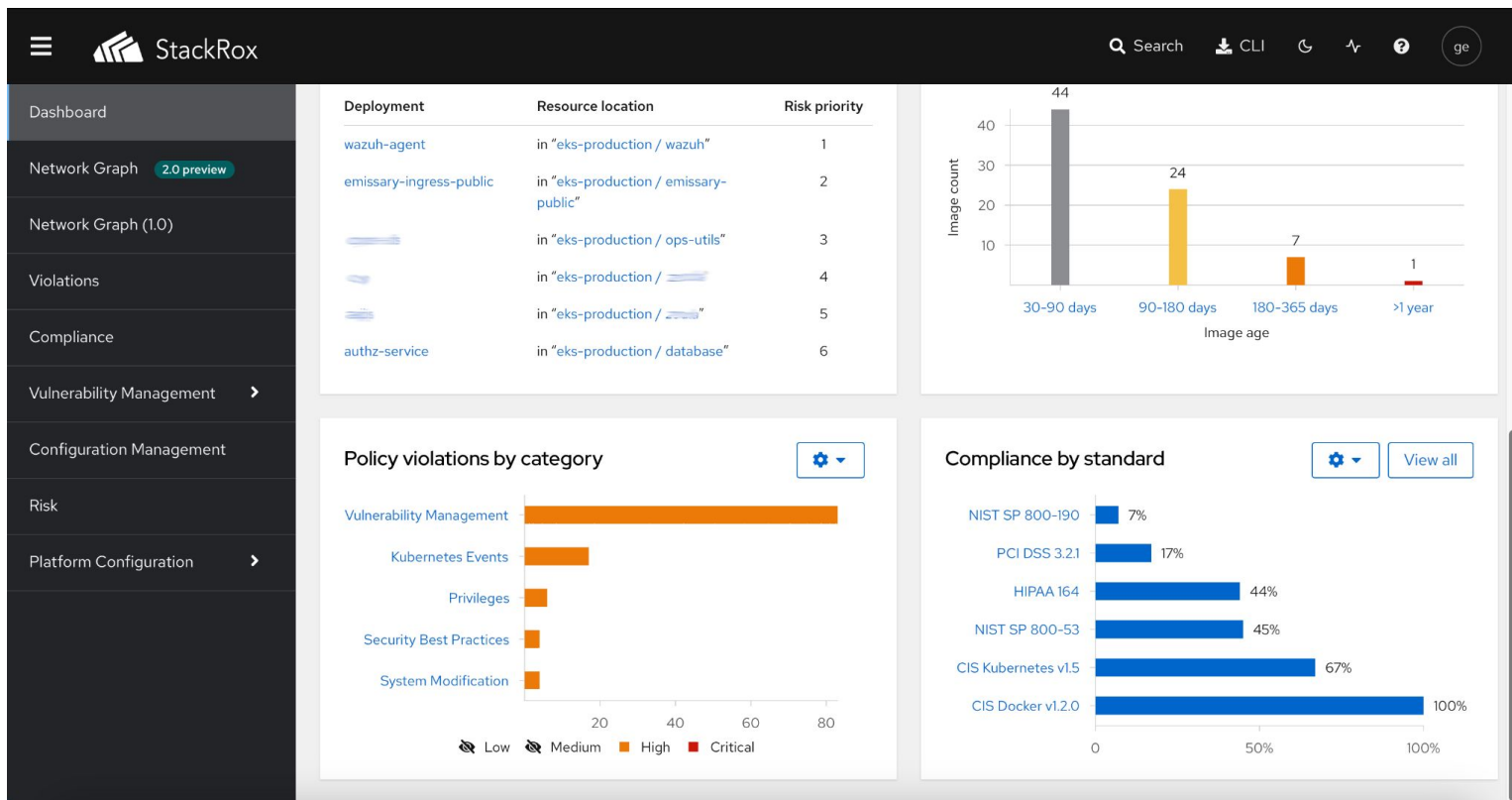
Notifier Integrations

slack Slack	StackRox Generic Webhook	Jira Software Jira	email Email
Google Cloud Platform Google Cloud SCC	splunk > Splunk	pagerduty PagerDuty	sumo logic Sumo Logic
Microsoft Teams	AWS Security Hub AWS Security Hub	Syslog Syslog	

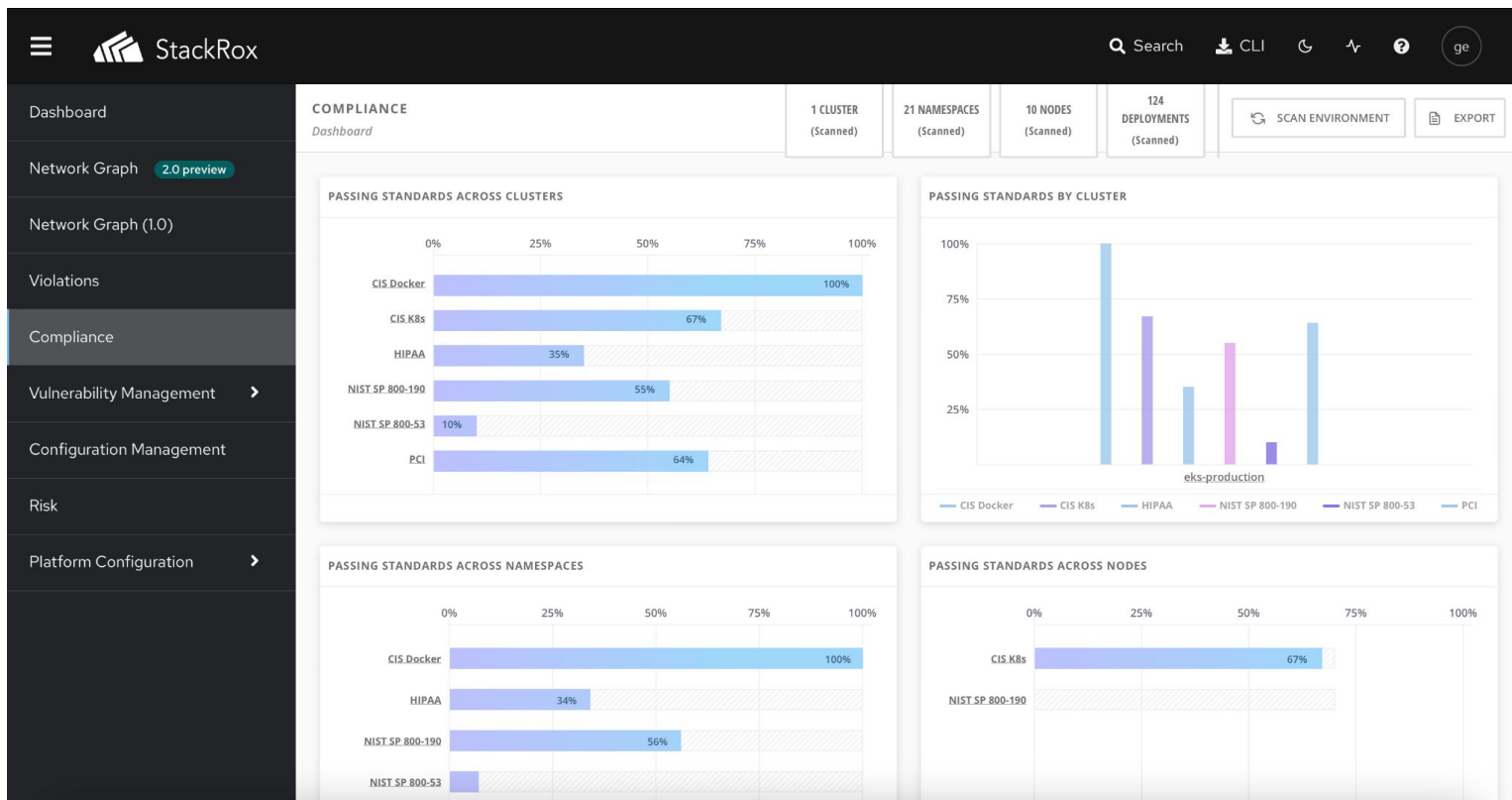
Дашборг



Дашборг



Дашборг



Kapma cemu

The screenshot displays the StackRox Network Graph interface. The top navigation bar includes the StackRox logo, a search bar, and icons for CLI, refresh, and help. The breadcrumb trail shows the current view: `eks-production` Namespace `5` Deployments.

The main area shows a network graph with nodes representing services and their connections. The nodes include:

- `cert-manager-webhook` and `cert-manager-cainjector` (grouped as `cert-manager`)
- `notification-controller`
- `ww-gitops-weave-gitops` and `kustomize-controller`
- `image-automation-controller`
- `source-controller` and `image-reflector-controller`
- `helm-controller` (labeled `443/TCP`)
- `flux-system`

External entities like `Cloudflare`, `External Entities`, and `Amazon/GLOBAL` are shown at the bottom of the graph.

The right sidebar is titled `Cloudflare` with IP `172.64.0.0/13`. It contains a search bar for filtering by entity name and a table of active flows:

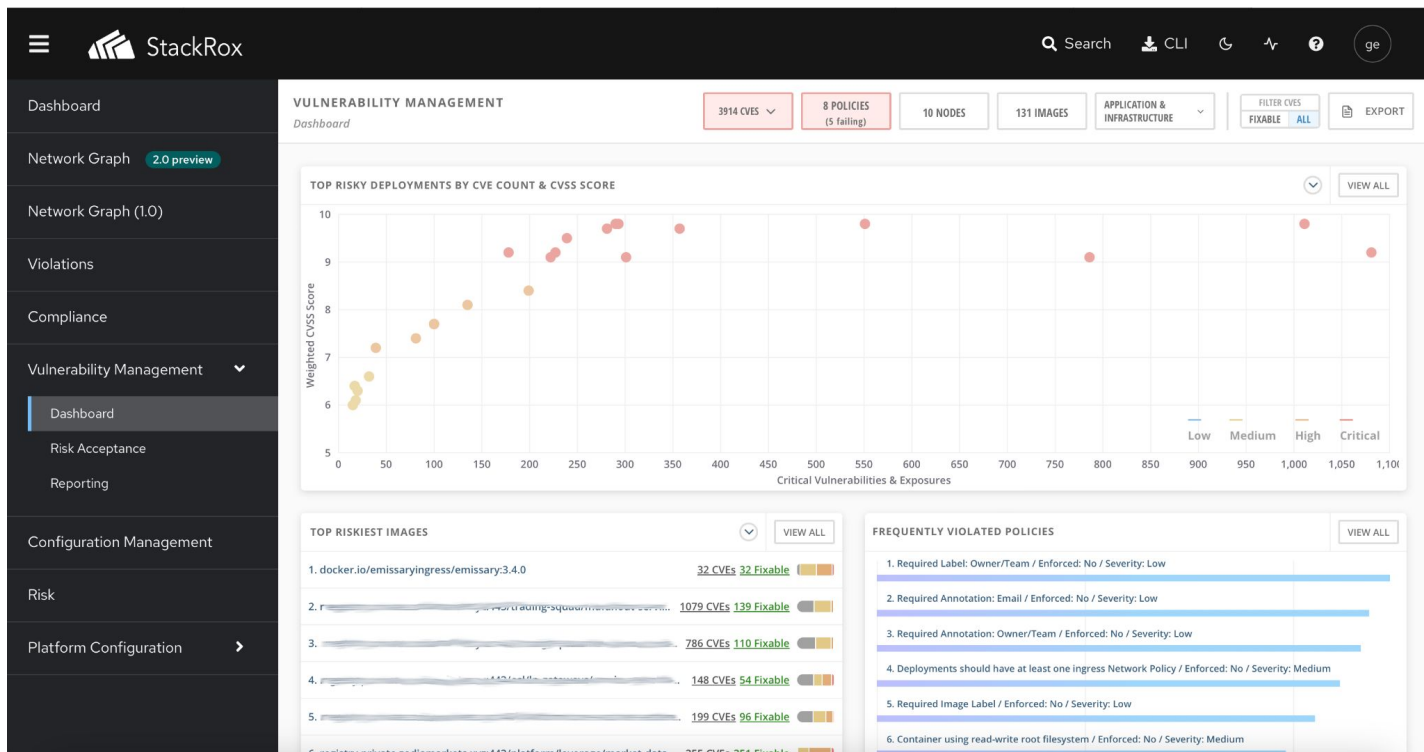
Entity	Direction	Port / protocol
<code>cert-manager</code> in "cert-manager"	Ingress	443 / TCP
<code>source-controller</code> in "flux-system"	Ingress	443 / TCP

Нарушения политик

The screenshot displays the StackRox web interface. The top navigation bar includes a menu icon, the StackRox logo, and utility icons for search, CLI, refresh, and user profile. The left sidebar lists navigation options: Dashboard, Network Graph (2.0 preview), Network Graph (1.0), Violations (selected), Compliance, Vulnerability Management, Configuration Management, Risk, and Platform Configuration. The main content area is titled 'Violations' and shows a filter for 'Namespace: kube-system'. It reports '2 results found' and displays a table of violations.

<input type="checkbox"/> Policy	Entity	Type	Enforced	Severity	Categories	Lifecycle	Time
<input type="checkbox"/> ADD Command used instead of COPY	coredns in "eks-production/kube-system"	deployment	No	Low	Multiple	Deploy	08/10/2023 6:02:41AM
<input type="checkbox"/> Docker CIS 5.19: Ensure mount propagation mode is not enabled	ebs-csi-node in "eks-production/kube-system"	deployment	No	Medium	Docker CIS	Deploy	08/10/2023 6:01:41AM

Управление уязвимостями - 1



Управление уязвимостями - 2

The screenshot displays the StackRox vulnerability management interface. The left sidebar contains navigation options: Dashboard, Network Graph (2.0 preview), Network Graph (1.0), Violations, Compliance, Vulnerability Management (with sub-options: Dashboard, Risk Acceptance, Reporting), Configuration Management, Risk, and Platform Configuration. The main content area is titled 'docker.io/emissaryingress/emissary:3.4.0' and includes an 'EXPORT' button and 'ALL ENTITIES' dropdown. Below the title are tabs for 'OVERVIEW', 'DEPLOYMENTS', 'IMAGE COMPONENTS', and 'IMAGE CVEs'. The 'Image Summary' section is expanded, showing 'Image Summary' details and metadata. The 'DETAILS & METADATA' section includes: Risk priority: 1, Top CVSS: 9.8 (Scored using CVSS V3), SHA: sha256:99f97f1c60854055deb97f9d4bcb66c312a64c500fbd6affac0d79205ab42a42, Created: 01/03/2023 | 4:19:01PM, Scanner: Stackrox Scanner, Scan time: 09/05/2023 | 7:05:17AM, and Image OS: alpine:v3.15. The 'CVES BY CVSS SCORE' section features a donut chart with a total score of 32, broken down into: 2 rated as Critical, 13 rated as Important, 14 rated as Moderate, and 3 rated as Low. The 'TOP RISKIEST IMAGE COMPONENTS' section lists: 1. alpine-baselayout:3.2.0-r18 (No CVEs), 2. alpine-keys:2.4-r1 (No CVEs), 3. apk-tools:2.12.7-r3 (No CVEs), 4. bash:5.1.16-r0 (No CVEs), and 5. brotli:1.0.9-r5 (No CVEs). The 'Related entities' sidebar on the right shows: MATCHES (1 DEPLOYMENT), CONTAINS (33 IMAGE COMPONENTS), and 32 IMAGE CVEs. The 'Image Findings' section is also visible, with a sub-tab for 'Observed CVEs'.

Управление уязвимостями - 3

The screenshot displays the StackRox vulnerability management interface. The left sidebar contains navigation options: Dashboard, Network Graph (2.0 preview), Network Graph (1.0), Violations, Compliance, Vulnerability Management (expanded), Dashboard, Risk Acceptance, Reporting, Configuration Management, Risk, and Platform Configuration. The main content area shows the details for the image `docker.io/emissaryingress/emissary:3.4.0`. The interface includes tabs for OVERVIEW, DEPLOYMENTS, IMAGE COMPONENTS, and IMAGE CVES. A table lists 13 CVEs with columns for CVE ID, Fixable status, Severity, CVSS score, Affected components, and Discovered date. The severity levels are color-coded: Critical (purple), Important (red), and Medium (orange). A right-hand sidebar shows related entities: 1 DEPLOYMENT, 33 IMAGE COMPONENTS, and 32 IMAGE CVEs.

<input type="checkbox"/>	CVE	Fixable	Severity ↓	CVSS sco... ↑	Affected compone...	Discovered ↑	
<input type="checkbox"/>	CVE-2023-23914	Yes	Critical	9.1	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-37920	Yes	Critical	9.8	1 components	08/10/2023 3:06:19PM	⋮
<input type="checkbox"/>	CVE-2022-23491	Yes	Important	7.5	1 components	08/10/2023 3:06:19PM	⋮
<input type="checkbox"/>	CVE-2022-4450	Yes	Important	7.5	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-0215	Yes	Important	7.5	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-0286	Yes	Important	7.4	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-0464	Yes	Important	7.5	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-25577	Yes	Important	7.5	1 components	08/10/2023 3:06:19PM	⋮
<input type="checkbox"/>	CVE-2023-2603	Yes	Important	7.8	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-27533	Yes	Important	8.8	1 components	08/23/2023 7:05:17AM	⋮
<input type="checkbox"/>	CVE-2023-27534	Yes	Important	8.8	1 components	08/23/2023 7:05:17AM	⋮

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