

БЕЗОПАСНОСТЬ  
КОНТЕЙНЕРОВ  
И KUBERNETES: НЕ  
ПРОБЛЕМА,  
А РЕШЕНИЕ

**Дмитрий Евдокимов**

Основатель и технический директор Luntry



# Обо мне



Я не верю в то, что систему можно сделать надежной и безопасной, не понимая того, как она устроена.



## Основатель и технический директор **Luntry**

Более 15 лет опыта в ИБ

## Специализация – безопасность контейнеров и Kubernetes

Автор ТГ-канала [k8s\(in\)security](#)

## Эксперт в сфере безопасности контейнерных сред

- Организатор конференции «БеКон» по БЕзопасности КОНтейнеров
- Бывший редактор рубрик в журнале «ХАКЕР», автор серии статей
- Автор курса «Cloud Native безопасность в Kubernetes»
- Член программного комитета CFP DevOpsConf и HighLoad++

## Спикер

VK Kubernetes  
DevOpsConf  
Kazhackstan

Confidence  
HackInParis  
HighLoad++

ZeroNights  
KuberConf  
OFFZONE

БеКон  
BlackHat  
DevOps

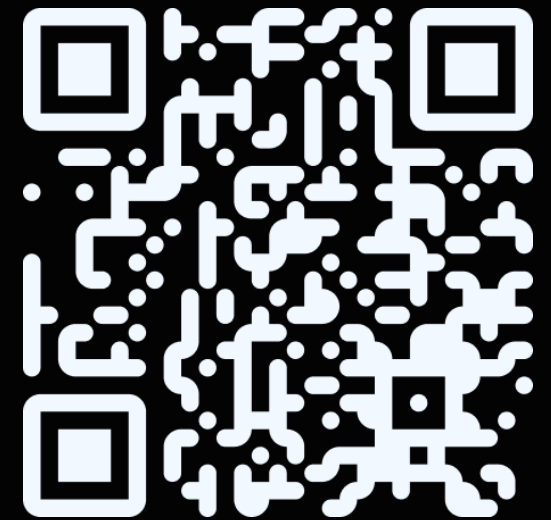
HITB  
PHDays  
SAS

# О компании Luntry

Luntry — это Комплексная Защита на всем жизненном цикле контейнерных приложений и средств оркестрации на базе Kubernetes

Продукт в реестре Минцифры  
<https://reestr.digital.gov.ru/reestr/1057835/>

Получение сертификата ФСТЭК планируется во втором квартале 2026 года.



# LUNTRY.RU

# Функциональность Luntry

---

Контроль всех  
Kubernetes-ресурсов

---

Контроль состояния Kubernetes-  
кластеров

---

Контроль соответствия кластера  
стандартам



**LUNTRY**



---

Управление уязвимостями  
образов и best practice

---

Сетевая безопасность

---

Анализ прав доступа

---

Защита Runtime

# Функциональность Luntry

---

Контроль всех  
Kubernetes-ресурсов

---

Контроль состояния Kubernetes-  
кластеров

---

Контроль соответствия кластера  
стандартам



**LUNTRY**



---

Управление уязвимостями  
образов и best practice

---

Сетевая безопасность

---

Анализ прав доступа

---

Защита Runtime

# Жизненный путь образа

## CI\CD Pipeline

- Сборка образа
- Анализ образа
- Security/Quality gates
  - Возможна блокировка
- Подпись образа

## Image registry

- Хранение
- Очистка/ротация
- Анализ образов
- Security/Quality gates

## Runtime

- Запуск
- Анализ образов
- Security/Quality gates

Shift Left Security



Shift Everywhere Security



Shift Right Security



Shift Down Security



# Жизненный путь образа

## CI\CD Pipeline

- Сборка образа
- Анализ образа
- **Security/Quality gates**
  - Возможна блокировка
- Подпись образа

## Image registry

- Хранение
- Очистка/ротация
- Анализ образов
- **Security/Quality gates**

## Runtime

- Запуск
- Анализ образов
- **Security/Quality gates**

Shift Left Security



Shift Everywhere Security



Shift Right Security



Shift Down Security



# Security/Quality Gates – ворота качества

## CI

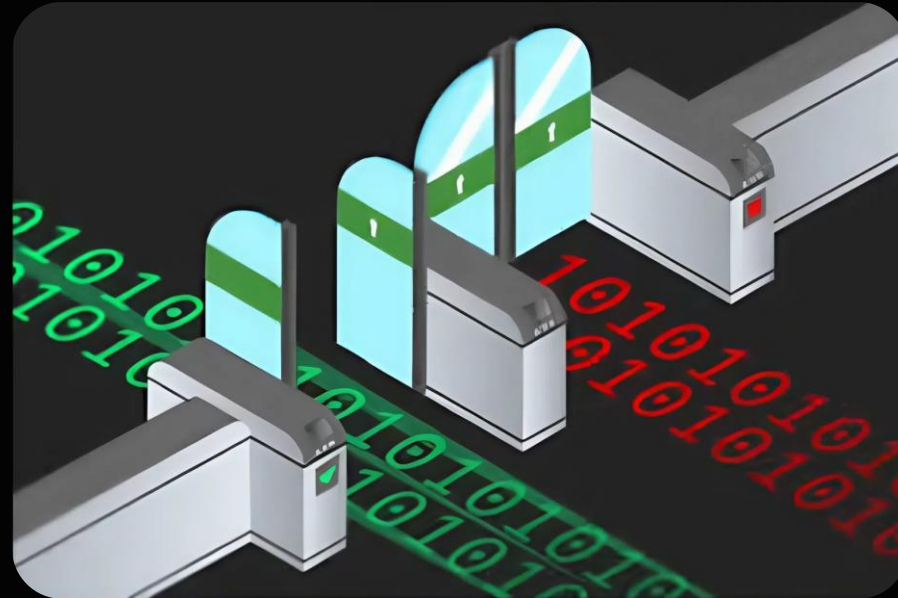
- Уведомление
- Блокировка

## Image registry

- Уведомление

## Runtime

- Уведомление



Блокировка на Deploy, Runtime – опасная и плохая практика!

[«Безопасность Kubernetes кластеров: вредные советы»](#), DevOpsConf 2024



# Домены безопасности образов

## 5 ДОМЕНОВ:

Анализ Dockerfile  
на лучшие практики

Поиск чувствительной информации

Анализ на известные  
уязвимости

Анализ на вредоносный код  
и код двойного назначения

Компонентный анализ





# Анализ образов в Luntry

- Встраивание в CI\CD, Registry, Runtime
- Инвентаризация использования образов
- Компонентный анализ (SBOM)
- Сканирование на известные уязвимости
- Поддержка отечественных ОС и БДУ ФСТЭК
- Приоритизация уязвимостей CVSS, Severity, Type(RCE/DoS), Exploit, KEV, EPSS, Runtime
- Контроль соответствия лучшим практикам
- Поиск секретов
- Анализ на вредоносный код и код двойного назначения
- Поддержка внешних и собственных IoC
- Встроенная библиотека уникальных проверок
- Скорость и парализация сканирований
- Security Gates в CI\CD, Registry, Runtime

Details Runtime Info SBOM **Vulnerabilities** Config Secrets Malware

Type: Vulnerability Report

Name: registry.k8s.io-ingress-nginx-controller-42b3f0e5

Updated: 10.04.2025 11:38:30

Registry: registry.k8s.io

Repository: registry.k8s.io/ingress-nginx/controller

Tag: sha256:42b3f0e5d0846876b1791cd3afeb5f1cbb4259d6f35651dcc1b5c980925379c

Total: 105

Fixed: 78

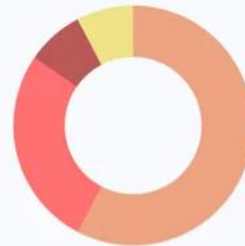
Exploit: 26

RCE: 1

DoS: 0

KEV: 0

[Report Components\(78\)](#) | [Components By Layers](#)



Summary

critical	6
high	21
medium	45
low	6
unknown	0
negligible	0

#	Name	CVEs	Fixable	Severity
1.	curl	14	14	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
2.	libcurl	14	14	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
3.	k8s.io/ingress-nginx	5	5	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
4.	libcrypto3	7	7	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
5.	libssl3	7	7	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
6.	openssl	7	7	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
7.	libxml2	4	4	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
8.	musl	1	1	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
9.	musl-utils	1	1	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>
10.	busybox-binsh	4	4	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>

Vulnerability Id	Severity	Type	Exploit	KEV	EPSS	Resource	Installed Version	Fixed Version
▼ CVE-2025-1974	critical	RCE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.99242	k8s.io/ingress-nginx	v1.10.0	1.11.5
<p>Description: ingress-nginx admission controller RCE escalation</p> <p>CVSS: • CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>Links:</p>								

Items per page: 10 1 - 400 of 1



# Security Gates в CI\CD, Registry, Runtime

Security Gates > Gates main

Runtime Policies | Policy Engines | Runtime Rules | Reaction Policies | Prevention Policies | Security Gates

Dashboard | Gates | Violations

Search...

Add gate +

Name	Severity	Scopes	Vuln	Sbom	Malware	Misconfig	Secret	Description	Block Action	Status
Many vulnerabilities	critical	CI/CD Registry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Images with more than 100 critical vulnerabilities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OS checks	critical	Registry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Check OS for vulnerabilities and malwares	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RCE and KEV	critical	Registry Runtime	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	images with RCE and KEV	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Secrets in pipeline	medium	CI/CD	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Block images with forgotten secrets in CI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Items per page: 25 1 - 25 of 4



# Пример 1: В CI

## Максимум экономии

на «самом дешёвом» этапе:

- Раннее обнаружение дефектов

## Экономика:

- Исправление проблемы на этапе CI дешевле, чем на последующих этапах

## Эффект на команду:

- Снижается нагрузка на QA/DevOps/SRE



Security Gates > Gates main

Runtime Policies | Policy Engines | Runtime Rules | Reaction Policies | **Security Gates** | Audit Rules

Dashboard | **Gates** | Results

Search...  Scope <sup>3</sup> Severity <sup>4</sup> Active Add gate +

Name	Severity	Scopes	Vuln	Sbom	Malware	Misconfig	Secret	Description	Block Action	Status
gate1	critical	CI/CD Registry Runtime	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	only 1 crit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
no libssl	critical	CI/CD Registry Runtime	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no libssl <= 1.1.1 allowed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
no malware	critical	CI/CD Registry Runtime	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no malware allowed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



# Пример 2: В Image Registry

## Снижение риска и затрат на масштабирование ошибок:

- Единая точка контроля

## Экономика:

- Снижает стоимость аудита / соответствия — упрощает проверки и перепроверки, сокращает ручной труд

## Эффект на команду:

- Снижение FTE на команду безопасности

Security Gates > Gates main

Runtime Policies | Policy Engines | Runtime Rules | Reaction Policies | Security Gates

Gates | Violations

Search...

Add gate +

Name	Severity	Scopes	Vuln	Sbom	Malware	Misconfig	Secret	Description	Block Action	Status		
Extra critical vulns	critical	Runtime	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Runtime vulns monitoring	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Test Gate	critical	CI/CD Registry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Blocks images with critical vulnerabilities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Test Gate 2	high	Runtime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Blocks images with malware	<input type="checkbox"/>	<input checked="" type="checkbox"/>		



# Пример 3: В Runtime

Фокусирование на действительно опасном и важном в текущий момент:

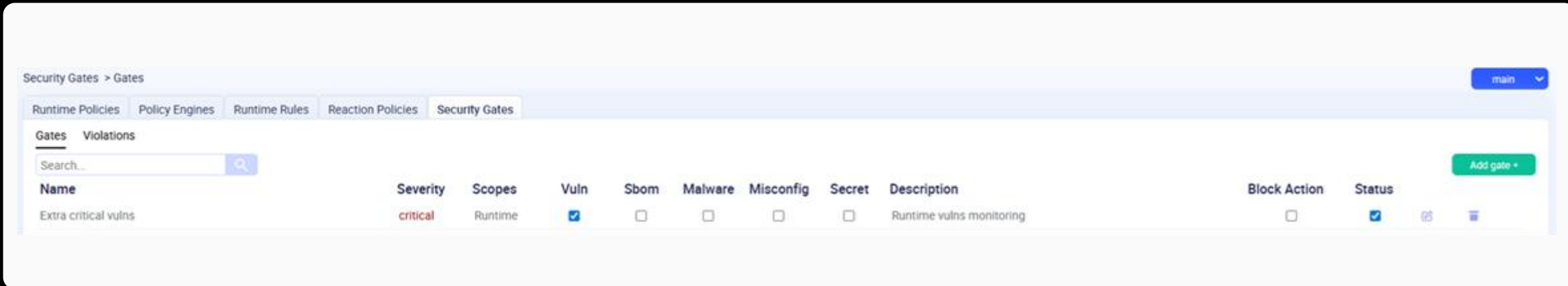
- Контроль самого актуального

Экономика:

- Экономия на инцидентах и простоях

Эффект на команду:

- Простота работы и понижения порога входа за счет приоритезации задач





# Польза Security Gates

## DEFENSE IN DEPTH:

- CI: «дешево исправить»
- Registry: «не дать распространиться»
- Runtime: «не дать навредить (или минимизировать ущерб)»

Ключевые бизнес-метрики, которые обычно улучшаются

- **Lead time / time-to-release**: меньше откатов и «красных» релизов.
- **Change failure rate**: снижается за счёт отсева дефектов и небезопасных изменений.
- **MTTR (время восстановления)**: ниже, потому что меньше инцидентов и выше прозрачность.
- **Стоимость владения (ТСО) платформы**: меньше ручных процессов, меньше «пожарных» часов, меньше потерь от downtime.



СПАСИБО ЗА ВНИМАНИЕ!



◀ [luntry\\_official](#)

◀ [luntrysolution](#)

▶ [luntrysolution](#)

🌐 [luntry.ru](#)

✉ [info@luntry.ru](#)

✉ [de@luntry.ru](#)

◀ [Qu3b3c](#)

◀ [k8security](#)

**Дмитрий Евдокимов**

Основатель и технический директор Luntry

