

«Синергия безопасности
Luntry и Штурвал. Часть 2»»



Дмитрий Евдокимов
Founder&CTO Luntry



Владимир Утратенко
BDM Штурвал

ДМИТРИЙ ЕВДОКИМОВ

”

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
DevOops

HITB
PHDays
SAS

Основной функционал Luntry

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

Контроль
Kubernetes-ресурсов

Контроль состояния
Kubernetes-кластеров

Контроль соответствия кластера
стандартам



LUNTRY

Управление безопасностью
образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime



ВЛАДИМИР УТРАТЕНКО

”

Верю и знаю, что тандем DevOps и K8s – это то, что будет ещё долгие годы двигать индустрию.



Менеджер
по развитию бизнеса
Штурвал, Лаборатория
Числитель

Экспертность
13 лет в IT, строил DevOps
и платформенные решения, когда
это ещё не было мейнстримом.

Эксперт в сфере DevOps и контейнеризации

- Прошёл путь от инженера поддержки до технического директора через DevOps и построение инфраструктуры
- Автор и ПК сообщества DevOps Moscow
- Член программного комитета Kuber community

Спикер

DevOps conf
HighLoad++
ProItFest

DevOpsDays
UIC.Dev
K8SDay

АЛЕКСАНДР КРЫЛОВ



Директор по
продвижению продукта
«Штурвал»

Экспертность
+12 лет в IT



Эксперт в сфере DevOps и контейнеризации

- Глава ПК и основатель Kuber community day, Observability conf
- Член ПК конференций: Merge, Стачка, ProITFest, Performance conf
- Автор курса «DevOps-инженер» в рамках проекта «Цифровые кафедры» для вузов РФ (МИРЭА, МГТУ, МГМУ, Станкин, ТГУ и других)

Спикер

DevOps conf
HighLoad++
TeamLead Conf

Industrial++
Стачка
Merge

ProITFest
DevOops

Платформа Штурвал

ШТУРВАЛ – Enterprise платформа управления K8s №1 в России*

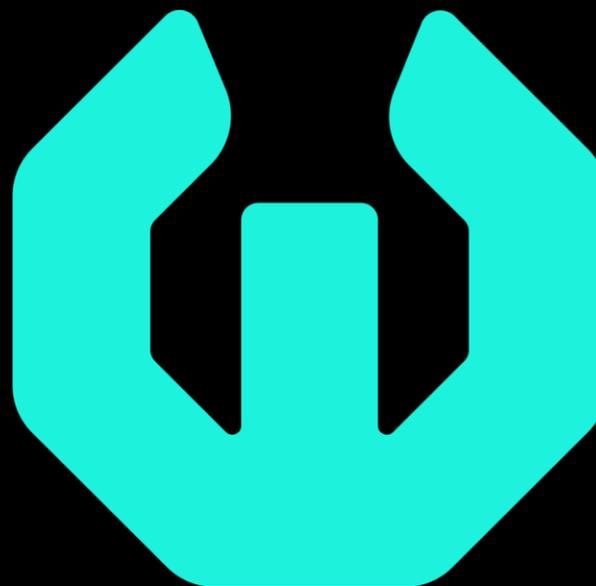
[*По версии рейтинга CNEWS](#)

Простой установщик K8s

Централизованное управление
множеством кластеров K8s

Гибкая сквозная ролевая
модель

Развёртывание и управление
в защищенных сегментах



Анализ конфигураций
и образов контейнеров
на уязвимости

Централизованное управление
политиками безопасности

Admission control

План вебинара

- 01 Введение
- 02 3 классических сценария
- 03 Выводы

Сегодняшние герои

Часть героев в Части 1 и еще будет Часть 3 😊

01

Обновление кластера

- Про поддержку кластера в актуальном, рабочем состоянии

02

Исправление уязвимостей в системных компонентах кластера

- Про обнаружение и исправление системных уязвимостей

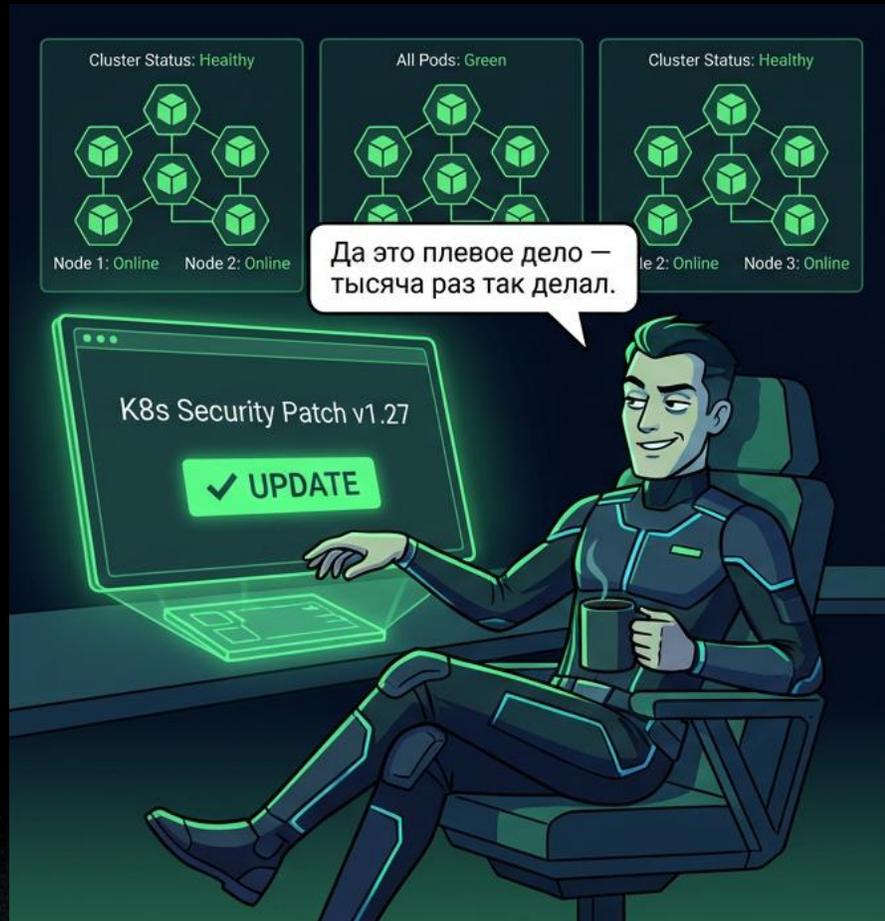
03

Безопасность образов контейнеров

- Про доверие и контроль к содержимому образов контейнеров

01 ОБНОВЛЕНИЕ КЛАСТЕРА

У всех так бывает #1



Нет нерешаемых проблем #1

Проблема

Сообщество Kubernetes поддерживает только 3 последних релиза. Остальные релизы не получают: обновлений, улучшений, исправлений

Вы не сможете поправить какие-то ошибки или получить какие-то важные улучшения, что может привести к проблемам эксплуатации.



Решение

Нужно уметь отслеживать цикл поддержки и быстро, надежно обновлять кластер.

Синергия в обновлениях



LUNTRY

Контроль актуальности
версий



Штурвал

Быстрота
обновления

ПОСТОЯННАЯ АКТУАЛЬНОСТЬ

Мы позволяем контролировать и быстро обновлять Kubernetes кластера.

Уходим от легаси к современным фичам и их преимуществам.

02 ИСПРАВЛЕНИЕ УЯЗВИМОСТЕЙ В СИСТЕМНЫХ КОМПОНЕНТАХ КЛАСТЕРА

Нет не решаемых проблем #2

Проблема

В системных компонентах Kubernetes тоже есть уязвимости. И их несвоевременное исправление может привести к инциденту.

Нужно компоненты быстро обновлять или соответствующим образом митигировать.



Решение

Отслеживание фида уязвимостей системных компонентов с пониманием риска.

Синергия в обновлениях



LUNTRY

Информирование
об уязвимостях
в системных компонентах



Штурвал

Контроль
за компонентами

Контролируемая инфраструктура

Мы можем дать уверенность на уровне системы
о безопасности системных компонент.

03 БЕЗОПАСНОСТЬ ОБРАЗОВ КОНТЕЙНЕРОВ

У всех так бывает #3

Sigstore/Notary

Pod Service Pod Ingress Backend

Да какая разница, подписано или нет? Работает же, тащим!

SBOM

```
docker.io/library/untrusted-app:latest
```

⚠ SIGNATURE MISSING — VERIFY WITH COSIGN?

[IGNORE] [VERIFY]

Image policy: unsigned allowed | Cluster risk: elevated

Image compromise detected — malware: cryptominer, backdoor
RuntimeClass: malicious | Pod network breached
CVE-2025-ABCD — active exploit in unsigned base image

FAIL

FAIL

FAIL

CRASH

COMPROMISED

CRYPTO MINER

BACKDOOR

КЛАСТЕР ЗАРАЖЕН. ВСЕ НЕПОДПИСАННЫЕ ОБРАЗЫ — ЭТО ЛОВУШКА.

```
cosign verify -key
```

FAIL

Sigstore

Тащил что попало — вырастил монстра.
Без подписей образы не тащим.

Нет не решаемых проблем #3

Проблема

Для создания микросервиса разработчики берут что-то внешнее или собирают из множества сторонних компонентов (60-90%) без контроля насколько это безопасно.

Далее через это недоваренное получаем инцидент безопасности.



Решение

Необходим механизм, который даст уверенности в происхождении и соответствующем качестве разрабатываемых или приносимых образов контейнеров.

Синергия в контроле образов



LUNTRY

Сканер образов
Security Gates



Штурвал

Проверка подписи
образа

Безопасная разработка образов

Мы гарантируем то, что ничего плохого, непроверенного
не пройдет мимо.

ВЫВОДЫ

Выводы

01

Обновления это не страшно

02

Контроль системных компонент это просто

03

Безопасность образов из коробки

04

Luntry и Штурвал дополняют и усиливают друг друга



📌 [luntry_official](#)

🌐 [luntry.ru](#)

📰 [luntrysolution](#)

✉️ info@luntry.ru

📺 [luntrysolution](#)

📌 [shturval_community](#)

🌐 <https://chislitellab.ru/shturval>

📌 [l4_helper_bot](#)

✉️ Info@chislitellab.ru

📌 [kuber_community](#)

ДМИТРИЙ ЕВДОКИМОВ

Founder & CTO Luntry

✉️ de@luntry.ru

📌 [Qu3b3c](#)

📌 [k8security](#)

АЛЕКСАНДР КРЫЛОВ

СРО «Штурвала»

✉️ aa.krylov@chislitellab.ru

📌 [@darkbenladan](#)