LUNTRY

«Синергия безопасности Luntry и Штурвал. Часть 1»



Дмитрий Евдокимов
Founder&CTO Luntry



Владимир Утратенко
менеджер по развитию бизнеса Штурвал

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

LUNTRY

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	Confidence	ZeroNights	БеКон	HITB
DevOpsConf	HackInParis	KuberConf	BlackHat	PHDays
Kazhackstan	HighLoad++	OFFZONE	DevOops	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

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

LUNTRY | штурвал

Сегодняшние герои

Остальные переехали в вебинар Часть 2 ☺

01

Доступы и права

• Про пользователей, группы, ServiceAccounts

02

Сетевая безопасность

• Про сеть, ее сегментацию и микросегментацию

03

Мультитенантность и контроль YAMLs

• Про окружения и их влияние друг на друга

01 ДОСТУПЫ И ПРАВА

У всех так бывает #1



Нет не решаемых проблем #1

Проблема

Кластер Kubernetes очень динамическая среда, которой пользуются множество команд, и которая постоянно эволюционирует.

Так что потом сложно сказать что действительно надо, а что можно смело убирать. А все это увеличивает поверхность атаки и вероятность инцидента.



Решение

Нужно уметь следить кто что умеет делать в кластере и к чему это может привести.

Синергия в контроле полномочий

LUNTRY | штурвал

Анализ RBAC
Библиотека опасных прав
Конструктор проверок

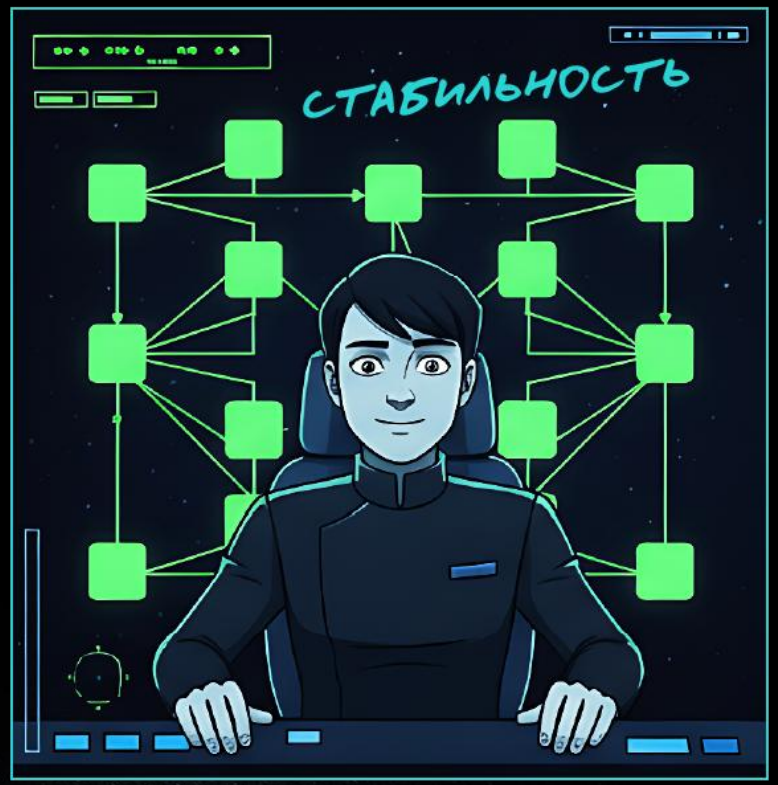
Дерево доступов

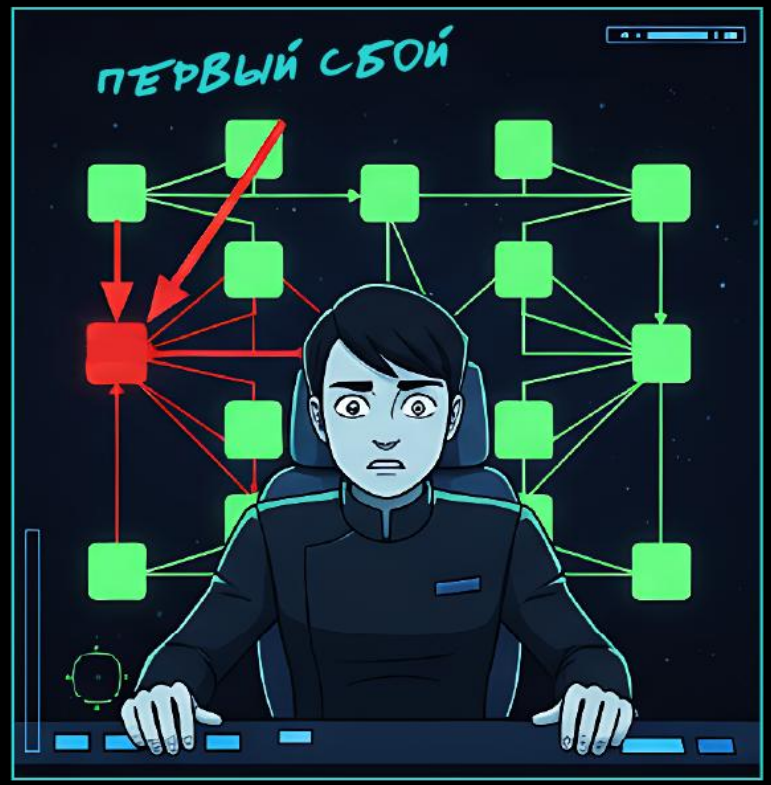
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

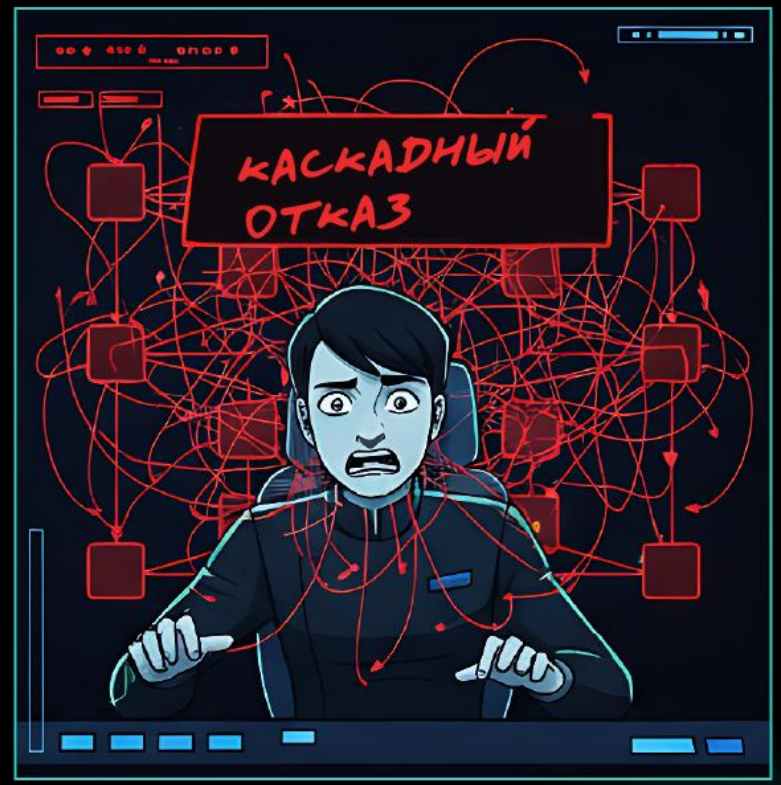
Мы позволяем контролировать и наводить порядок
с правами субъектов в любой момент времени.
Уходим от хаоса к принципу наименьших привилегий.

02 СЕТЕВАЯ БЕЗОПАСНОСТЬ

У всех так бывает #2







Нет не решаемых проблем #2

Проблема

Уязвимости были, есть и будут. У атакующего также есть 0day, backdoor (НДВ), APT и т.д.

Нужно строить безопасность даже в реалиях плохой картины со всем этим.



Решение

Чтобы ограничить ущерб даже при успешной атаке, нам нужны внутренние «противопожарные стены».

В Kubernetes это сетевые политики (NetworkPolicy).

Синергия в сетевой безопасности





Карта сетевой активности
Генератор NetworkPolicy

CNI Cilium
Конструктор NetworkPolicy

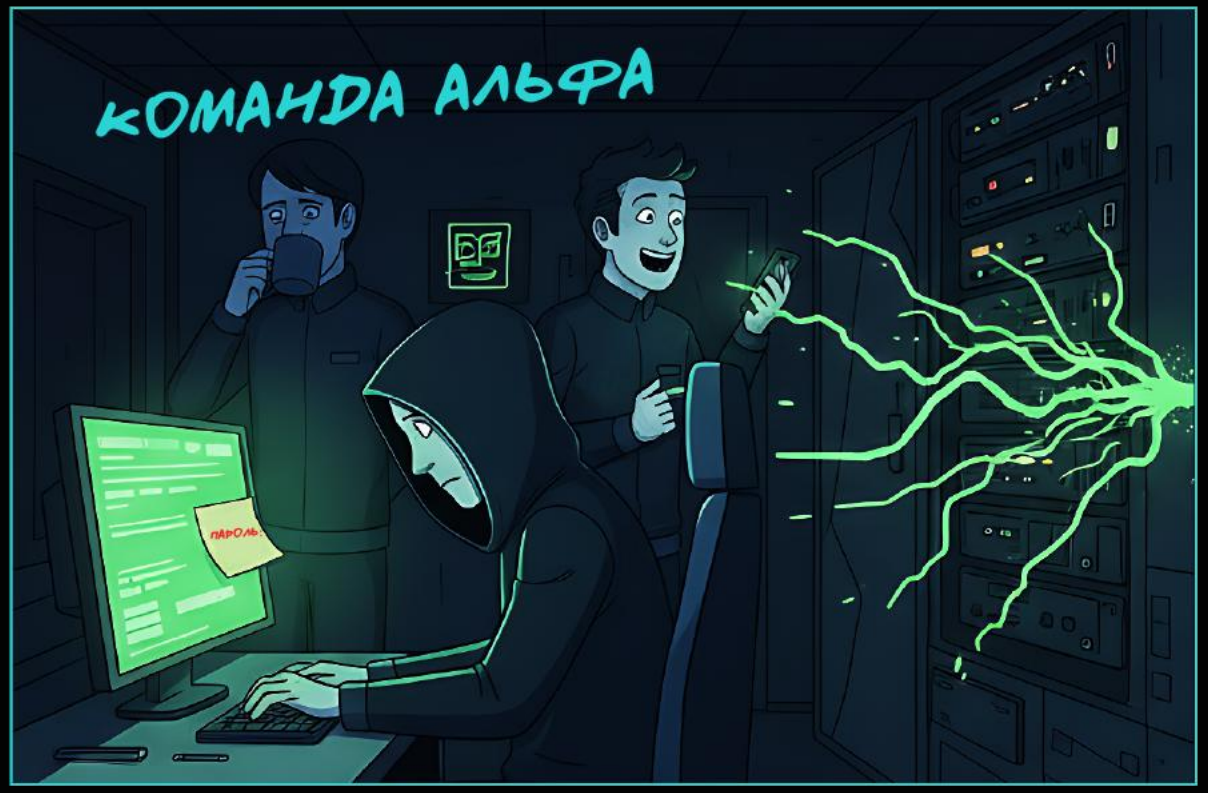
ZeroTrust

Мы можем построить стратегию «изоляции
и сдерживания» (Isolate and Contain) для микросервисов
как с найденными уязвимостями, не дожидаясь
их исправления, так и с неизвестными угрозами.

03 МУЛЬТИТЕНАНТНОСТЬ И КОНТРОЛЬ YAMLS

LUNTRY | штурвал

У всех так бывает #3





Нет не решаемых проблем #3

Проблема

Уязвимость / атака / инцидент
в одном проекте ставит
под угрозу безопасность
всего кластера
(риск «шумного соседа»).



Решение

Нам нужен механизм, который
создает безопасные
изолированные «комнаты»
для каждой команды,
где их проблемы остаются
их проблемами.

Синергия в изоляции команд и окружений





Анализ Kubernetes Audit Log
Библиотека детектов
PolicyEngine
Библиотека политик

Управление Kubernetes Audit Log
Концепция Тенантов

MULTITENANCY

Мы превращаем кластер из «общего общежития»
в «дом с изолированными квартирами», где инцидент
фиксируется и не приводит к катастрофе для всех.

ВЫВОДЫ

Выводы

01 Хаос с правами можно обуздать

02 Сетевая безопасность не такая страшная как ее рисуют

03 Изолированное окружение это право, а не привилегия

04 Luntry и Штурвал дополняют и усиливают друг друга

LUNTRY

luntry_official
luntrysolution
luntrysolution
luntry.ru
info@luntry.ru

ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ

LUNTRY | штурвал