tech LUNTRY

5 способов потерять кластер Kubernetes

Угрозы, о которых вспоминают слишком поздно



Алексей Волков

Лидер направления Developer Productivity в VK Cloud, VK Tech



Дмитрий Евдокимов

Founder & CTO Luntry

Обо мне



Алексей Волков

Лидер направления
Developer Productivity
в VK Cloud, VK Tech

Экспертность

В ИТ более 20 лет.
Эксперт по Kubernetes, облачному резервному копированию и IaC.

Опыт

10 лет работает с облачными технологиями AWS, Azure, Google. До VK Tech участвовал в развитии ПО для облачного резервного копирования. Создал и возглавил Client Onboarding отдел. Разработал PowerShell модуль, который позволил разворачивать облачный бекап в сложных Enterprise сценариях.

Спикер на конференциях HighLoad++, VK Kubernetes Conf и вебинарах VK Cloud.
Сертифицированный AWS Solution Architect Associate.
Cloud Champion 2023, номинант программы признания VK Tech 2023.

Принимал участие в экспертной команде помощи в запуске нового сервиса BI-системы на 25 000 клиентов.

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

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

Поговорим о реальных инцидентах, связанных со следующими причинами

1. Аспект хостовой ОС кластера
2. Проблемы настройки Kubernetes
3. YAML-ресурсы K8s
4. Безопасность образов
5. Контейнеры

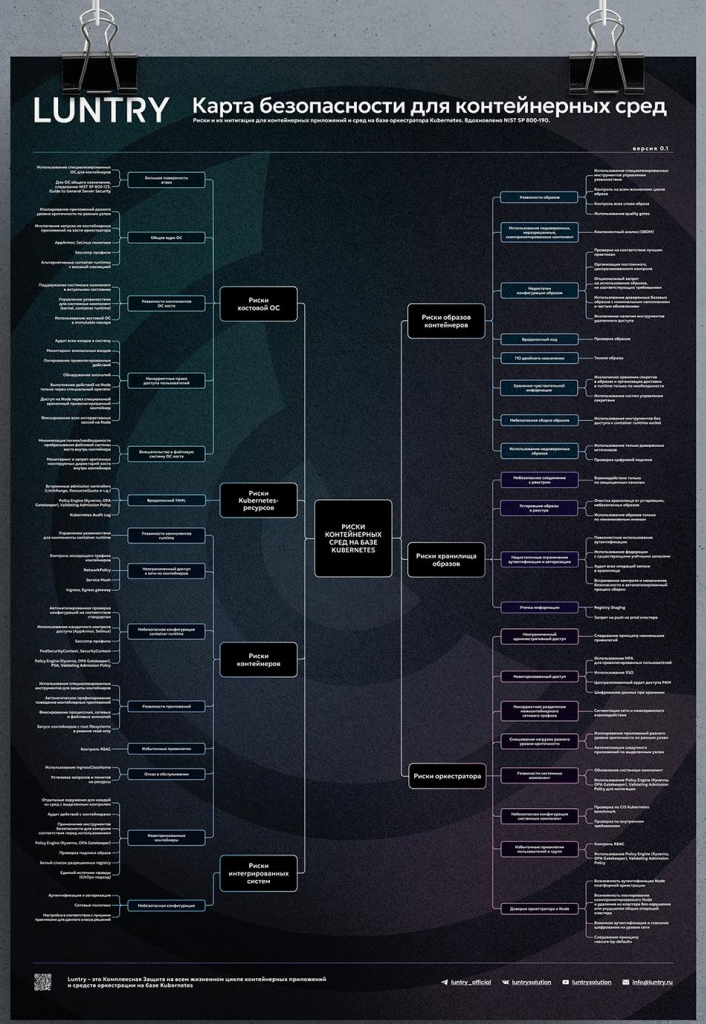
Карта безопасности для контейнерных сред

Версия от Luntry, с учетом NIST SP 800-190

Что это?

Эта карта, построенная на базе NIST SP 800−190 — позволит специалистам по безопасности, DevOps и SRE упростить восприятие картины рисков в целом.

Карта предоставляет структурированный подход к идентификации рисков и внедрению конкретных технических и организационных мер контроля для построения безопасной контейнерной платформы.



tech LUNTRY

Кейс 1

Вмешательство

в файловую систему ОС хоста

Почему монтирование системных директорий внутрь контейнера — опасная практика?

Кейс 2

Риски оркестратора: избыточные привилегии пользователей и групп

Как неправильная настройка прав превращает кластер в «проходной двор»?



Кейс 3

Риски Kubernetes-ресурсов: вредоносный YAML и слепые зоны

Как один YAML способен запустить цепочку инцидентов?



Кейс 4

Риски образов контейнеров: недоверенные образы и цепочки поставок

Почему скачивание «удобного» образа из непроверенного репозитория может стоить безопасности всей инфраструктуры?

Кейс 5

Риски контейнеров:

уязвимости приложений

Когда атака на приложение может проникнуть глубже — к данным и инфраструктуре?



Спасибо
за внимание



Алексей Волков

Лидер направления Developer Productivity
в VK Cloud, VK Tech



Дмитрий Евдокимов

Founder & CTO Luntry

de@luntry.ru

Qu3b3c

k8security

VK Cloud

LUNTRY

tech LUNTRY