itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

ЗАЩИТА AI-ИНФРАСТРУКТУР

Дмитрий Евдокимов
Основатель
и технический директор Luntry

LUNTRY

ITSEC 2026

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 KuberConf от АОТ

Спикер

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

LUNTRY

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/

Сертификат ФСТЭК России № 5116 от 30.09.2026 г

LUNTRY.RU

Функциональность Luntry

Контроль всех Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам



Управление безопасностью образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

LUNTRY

ВВЕДЕНИЕ

Разноплановая AI безопасность

LUNTRY

Безопасность AI

защищаем AI-системы
и их lifecycle

Безопасность от AI

защищаем компанию /
пользователей
от злоупотребления AI

Безопасность с AI

используем AI
как инструмент безопасности

Безопасность AI

- **AI Infrastructure Security**
  - hardware, GPU, cluster, storage, network
- **AI Supply Chain & MLOps Security**
  - pipelines, registries, checkpoints, dependencies
- **AI Data & Privacy Security**
  - datasets, labeling, provenance, DLP, retention
- **Model / LLM Security**
  - adversarial ML, extraction, robustness, safety bypass
- **Inference / App / RAG / Agent Security**
  - serving, prompts, retrieval, tools, action controls
- **AI-Generated Code / SDLC Security**
  - secure use of AI in engineering
- **Governance / Third-party / Compliance**
  - policy, audit, vendor management

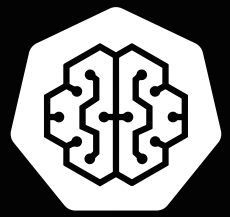
LUNTRY

Kubernetes (K8s)

Оркестратор	Стандарт де-факто для управления контейнеризированной нагрузкой
Обеспечивает надежную и масштабируемую среду для обработки больших данных	Big Data-ворклоады (например, с использованием Hadoop, Spark или AI/ML-пайплайнов) в Kubernetes увеличивают сложность системы • Volume (Объем) • Velocity (Скорость) • Variety (Многообразие)



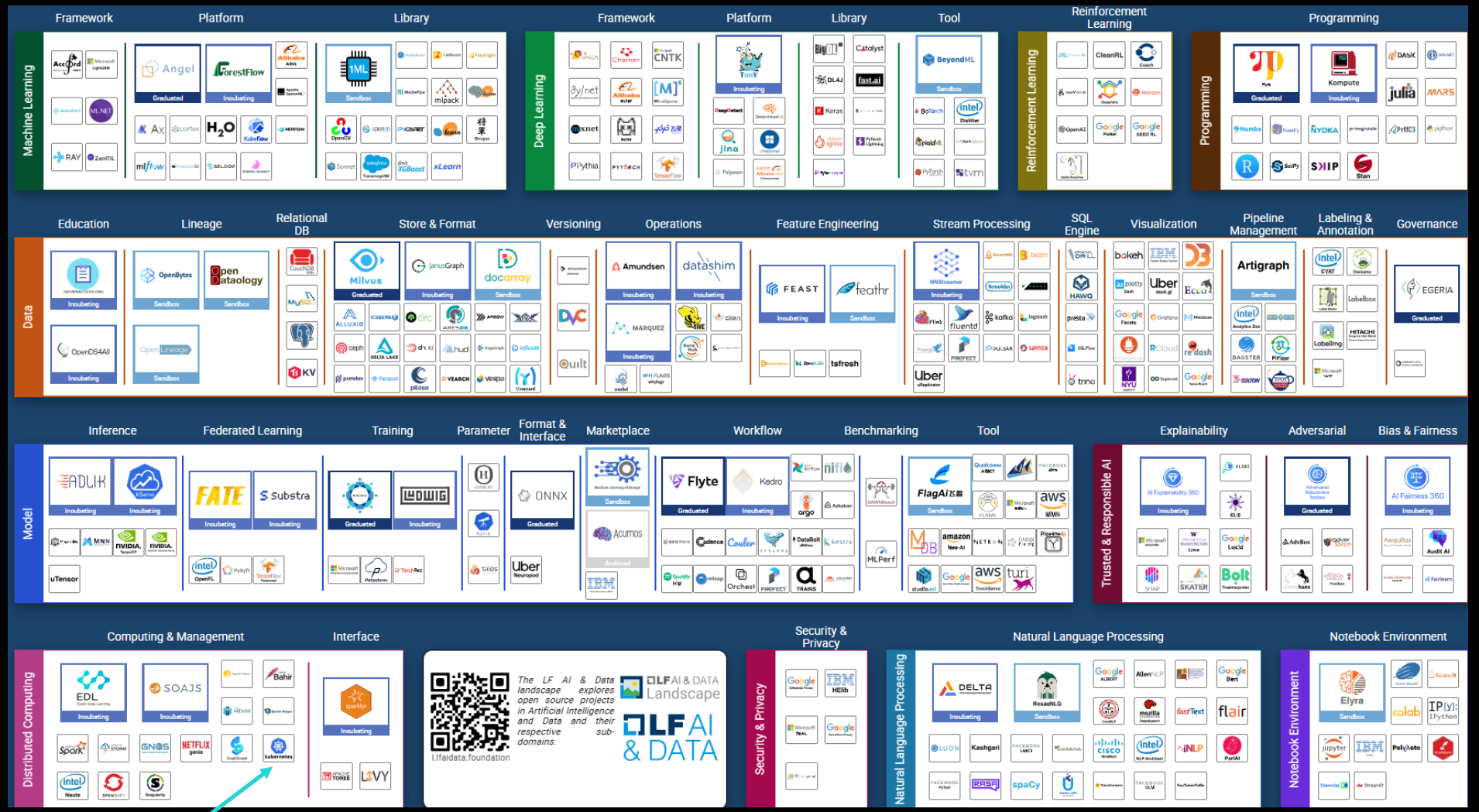




Kubernetes
AI DAY
EUROPE

LUNTRY

Kubernetes для задач AI и Data



Kubernetes

[LF AI & Data Foundation Interactive Landscape]

LUNTRY

K8s продолжает адаптироваться для AI

LUNTRY

Node Feature Discovery (NFD)

Данный проект призван помочь определить совместимость образа с конкретной конфигурацией хостовой ОС.

Ведь Nodes в кластере могут отличаться друг от друга:

- Драйверами
- Библиотеками и специализированным ПО
- Фичами ядра

Container Device Interface (CDI)

Спецификация для container runtimes, для поддержки разных сторонних устройств через общепринятую, понятную всем систему плагинов.

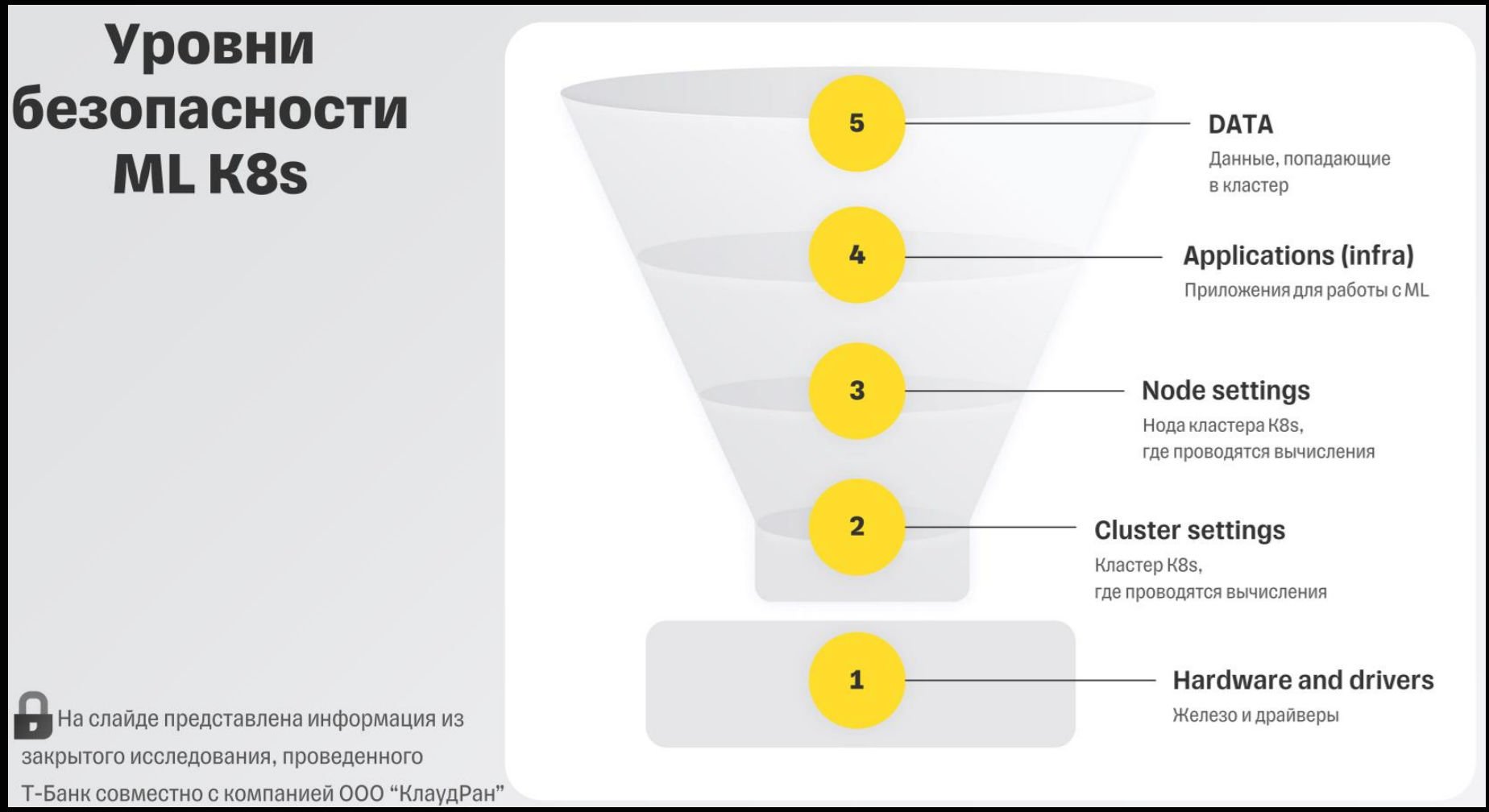
Механизм Checkpoint/Restore

Ускорение старта тяжёлых приложений, пауза и возобновление длительных вычислений (ML, batch-задачи), а также более эффективное использование ресурсов кластера.

LUNTRY

СПЕЦИФИКА БЕЗОПАСНОСТИ

Безопасность AI кластеров Kubernetes



"Чеклист безопасности ML-кластеров", Николай Панченко

Соответствие стандартам

- Big Data может добавить сложность для compliance из-за обработки чувствительных данных (PII, регуляторные требования как GDPR или PCI-DSS)



"Чеклист безопасности ML-кластеров", Николай Панченко

Управление безопасностью образов

LUNTRY

Big Data-ворклоуды используют сложные образы с множеством зависимостей (например, для аналитики или ML-фреймворков)

Характеристики:

- Очень большой размер
- Множество зависимостей
- Множество уязвимостей

Уязвимости NVIDIA Container Toolkit

LUNTRY

ОЧЕНЬ МНОГО УЯЗВИМОСТЕЙ:

- CVE-2025-23266 (CVSS Score 9.0)
- CVE-2025-23359 (CVSS Score 8.3)
- CVE-2024-0132 (CVSS Score 9.0)
- …

ХАРАКТЕРИСТИКИ:

- Очень простая и стабильная эксплуатация для побега из контейнера.
- Специально сформированный Dockerfile.

Нужно проверять как можно раньше!

Сетевая безопасность

LUNTRY

- Big Data генерирует огромный east-west трафик
  - Pod-to-Pod коммуникации для data ingestion, preprocessing и синхронизации моделей
- Big Data-ворклоады часто развертываются в нескольких кластерах
  - Например, отдельные для тренинга и инференса AI
- Сторонние сетевые решения по безопасности, которые стоят в разрыве, очень негативно влияют на производительность!
  - Никаких DPI, DLP и т.д.
- Native NetworkPolicy (Layer 3/4) хороши с точки зрения производительности, но их может не хватить для гранулярности
  - Например, недостаточны для контекстного контроля. Например, FQDN-фильтрации для внешних API.
  - Нужны Custom Network Policy от Cilium, Calico, Antrea

Необычные атаки и “фичи”

What are Shadow Vulnerabilities?

A pattern we found in many popular open source libraries.

Vulnerabilities that do not have a CVE assigned
- Or the CVE that was “Disputed”

Usually known to the maintainer
- “It is your responsibility to use it right”
- Intended behavior: “Vulnerable-by-design”

Silent misconfigurations

Mentioning them in the doc
- (which no one reads)



"Shadow Vulnerabilities in AI/ML Data Stacks - What You Don’t Know CAN Hurt You", Avi Lumelsky, Nitzan Mousseri

Мониторинг за контейнером

LUNTRY

Big Data подразумевает long-running процессы (аналитика, ML-джобы).

Следим как обычно за:

- Процессными событиями
- Сетевыми операциями
- Файловыми операциями

Строим профили нормального поведения.

Это требует особой обработки, иначе сенсор просто не справится с обработкой событий для детектирования атаки и будет потреблять большое количество ресурсов.

LUNTRY

ВЫВОДЫ

Выводы

01

AI-специфика влияет на безопасность в Kubernetes, в основном усиливая существующие вызовы и вводя новые риски.

02

AI в основном усиливает существующие вызовы и вводит новые риски и угрозы.

03

AI не отменяет того, что делается для классических кластеров — необходим комплексный подход к безопасности.

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Спасибо за внимание!

Вопросы?

Дмитрий Евдокимов

de@luntry.ru

Qu3b3c

k8security