LUNTRY

Безопасность, AI, Kubernetes

Дмитрий Евдокимов
(Founder & CTO Luntry)

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 KUBER CONF

Спикер

VK Kubernetes
DevOpsConf
Kazhackstan

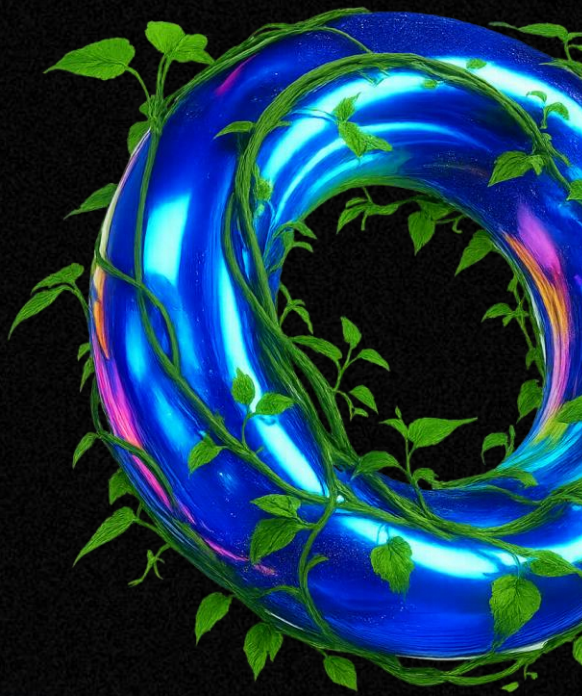
Confidence
HackInParis
HighLoad+
+

ZeroNights
KuberConf
OFFZONE

БеКон
BlackHat
DevOops

HITB
PHDays
SAS

СОДЕРЖАНИЕ

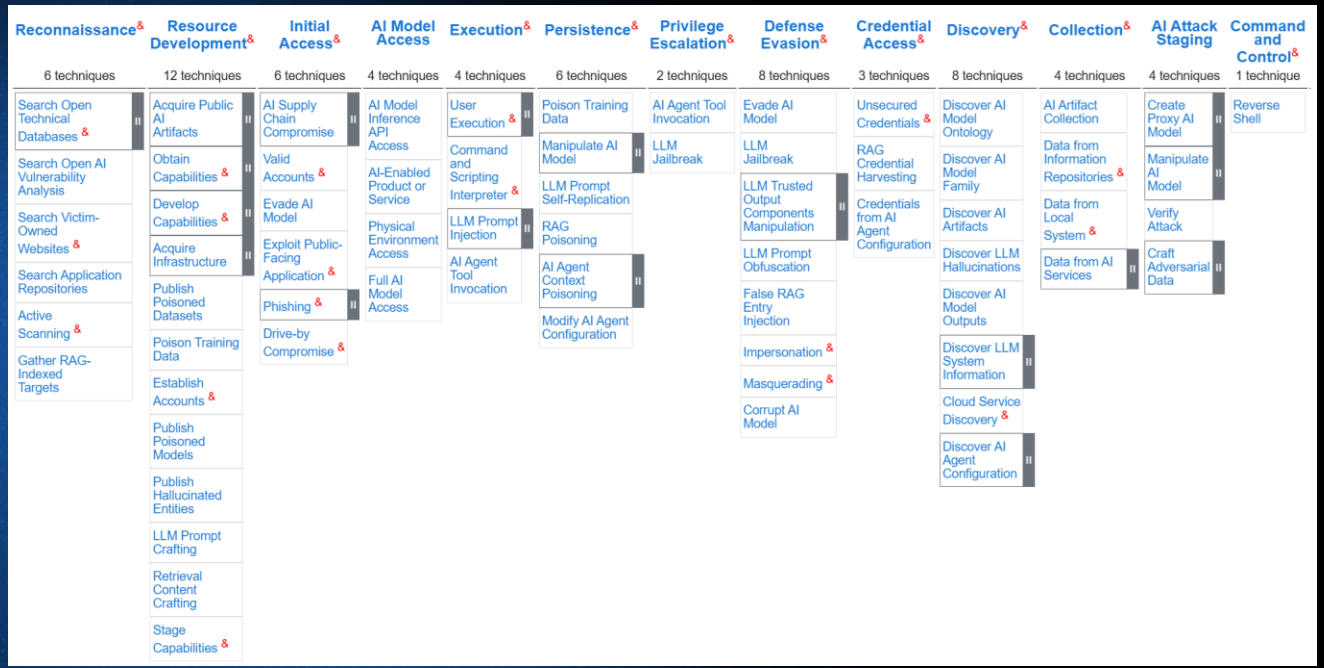


Главные герои

Безопасность

Безопасность AI

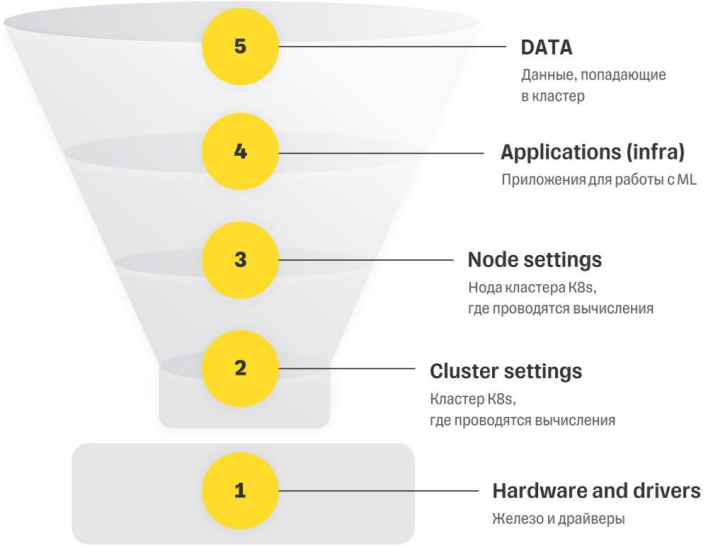
ATLAS Matrix



Безопасность

Безопасность AI кластеров Kubernetes

Уровни безопасности ML K8s

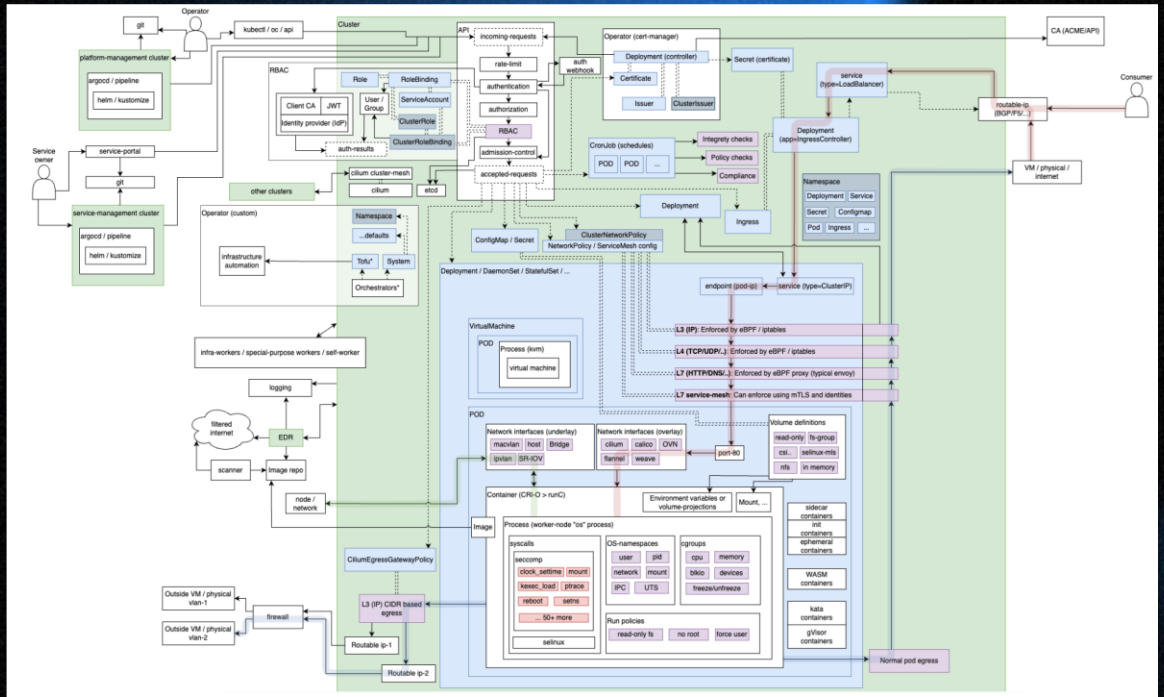


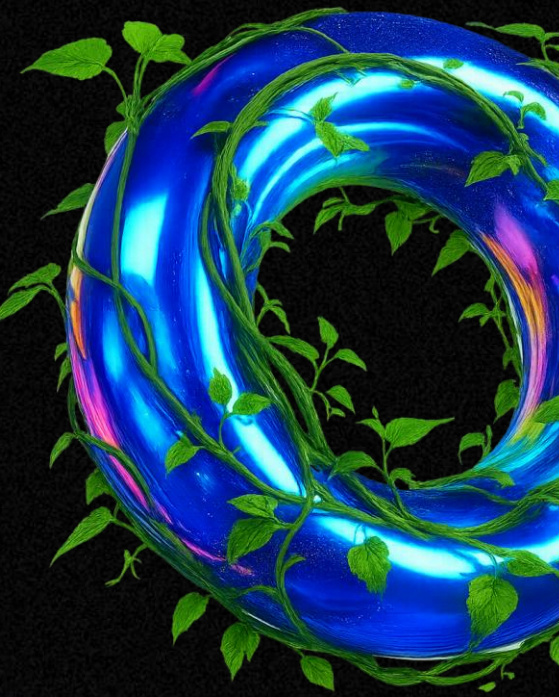
На слайде представлена информация из закрытого исследования, проведенного Т-Банк совместно с компанией ООО “КлаудРан”

"Чеклист безопасности ML-кластеров", Николай Панченко

Kubernetes

Kubernetes для задач безопасности

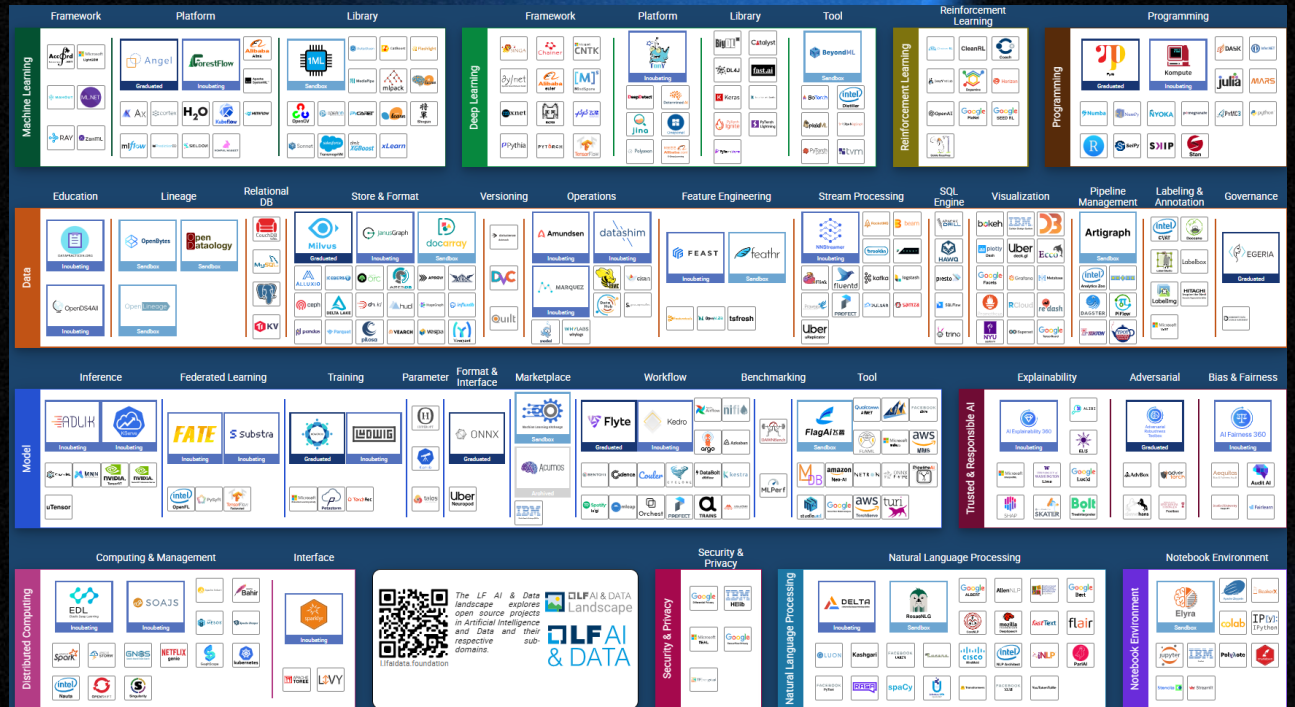




[Kubernetes security diagram (cheatsheet)]

Kubernetes

Kubernetes для задач AI



[LF AI & Data Foundation Interactive Landscape]

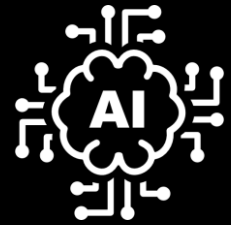
AI

AI в задачах безопасности

For the first time in bug bounty history, an autonomous penetration tester has reached the top spot on the US leaderboard.

[The road to Top 1: How XBOW did it]

AI



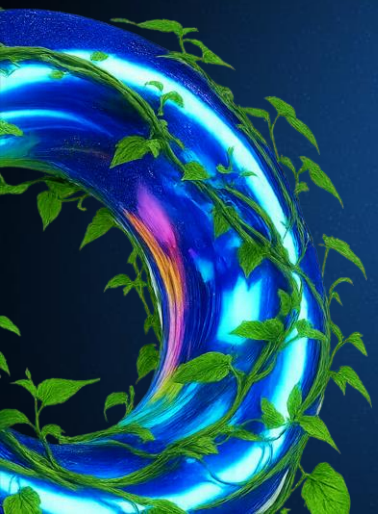
AI для безопасности Kubernetes

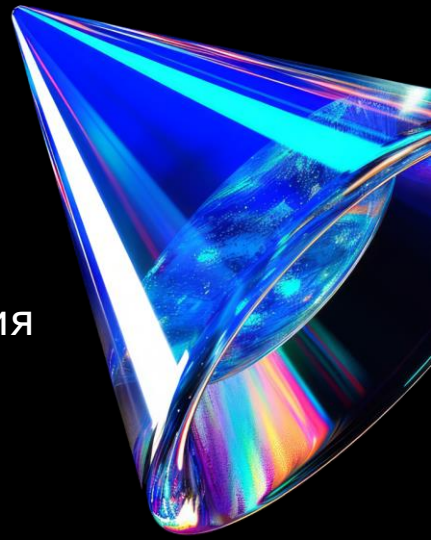
```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "l7-http-policy-example"
spec:
  endpointSelector:
    matchLabels:
      app: my-backend-service
  ingress:
  - fromEndpoints:
    - matchLabels:
        app: my-frontend-service
    toPorts:
    - ports:
      - port: "8080"
        protocol: TCP
      rules:
        http:
        - method: "GET"
          path: "/api/v1/status"
        - method: "POST"
          path: "/api/v1/submit"
```

"Kubernetes Resource Model (KRM): Everything-as-Code"

ВЫВОДЫ

1. Безопасность AI еще в стадии становления
2. Kubernetes стандарт дефакто
3. AI не всегда нужен и эффективен





В целом, эти технологии формируют экосистему, где AI ускоряет инновации, Kubernetes обеспечивает инфраструктуру, а безопасность — фундамент доверия.

СПАСИБО ЗА ВНИМАНИЕ!

de@luntry.ru

Qu3b3c

k8security

Дмитрий Евдокимов

LUNTRY