itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

КАК НЕ ЗАВАЛИТЬ SIEM В ВЫСОКОНАГРУЖЕННЫХ КЛАСТЕРАХ **KUBERNETES**

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

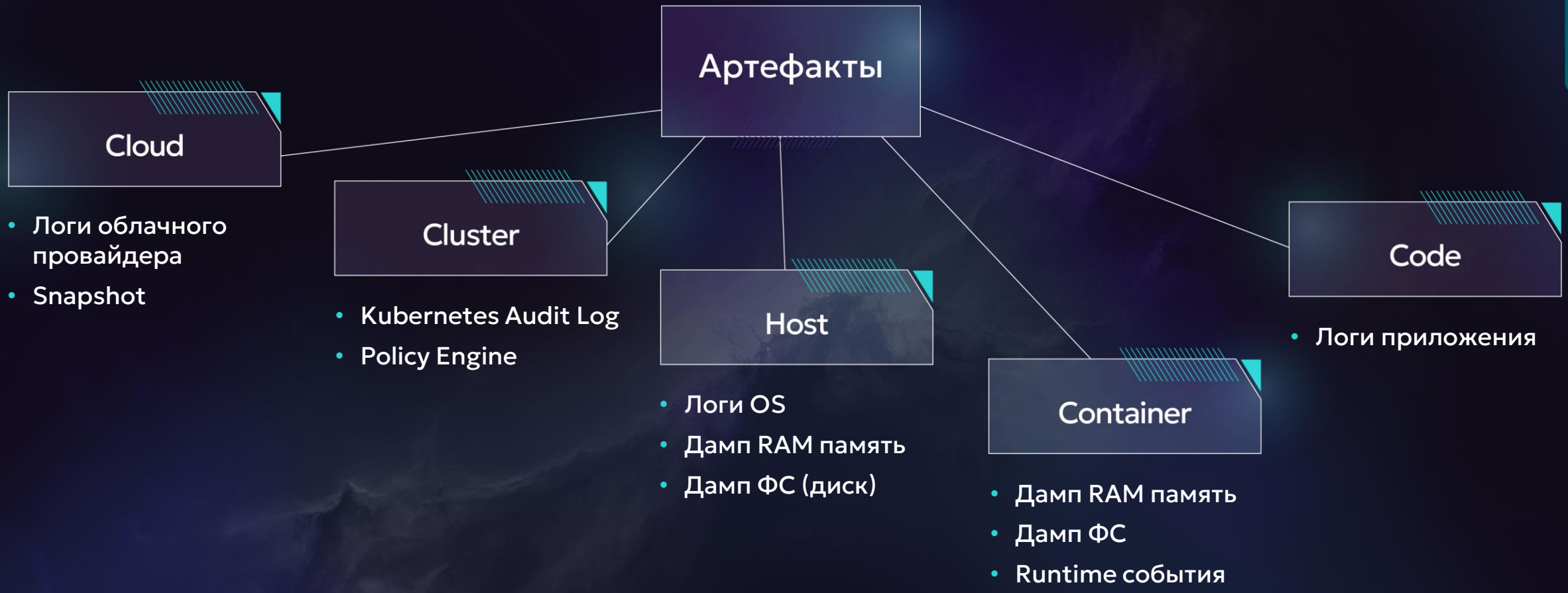
Классическая ситуация SOC с K8s

LUNTRY

Включили Kubernetes Audit Log, поставили runtime-агенты с 50 правилами, отправили всё в SIEM.

Потом начался rollout микросервиса.
Агент потребляет всё больше ресурсов, очередь растёт, события приходят с задержкой, происходят потери сообщений, а суточный лимит SIEM заканчивается раньше рабочего дня.

Источники данных в кластере K8s



- Логи облачного провайдера
- Snapshot

- Kubernetes Audit Log
- Policy Engine

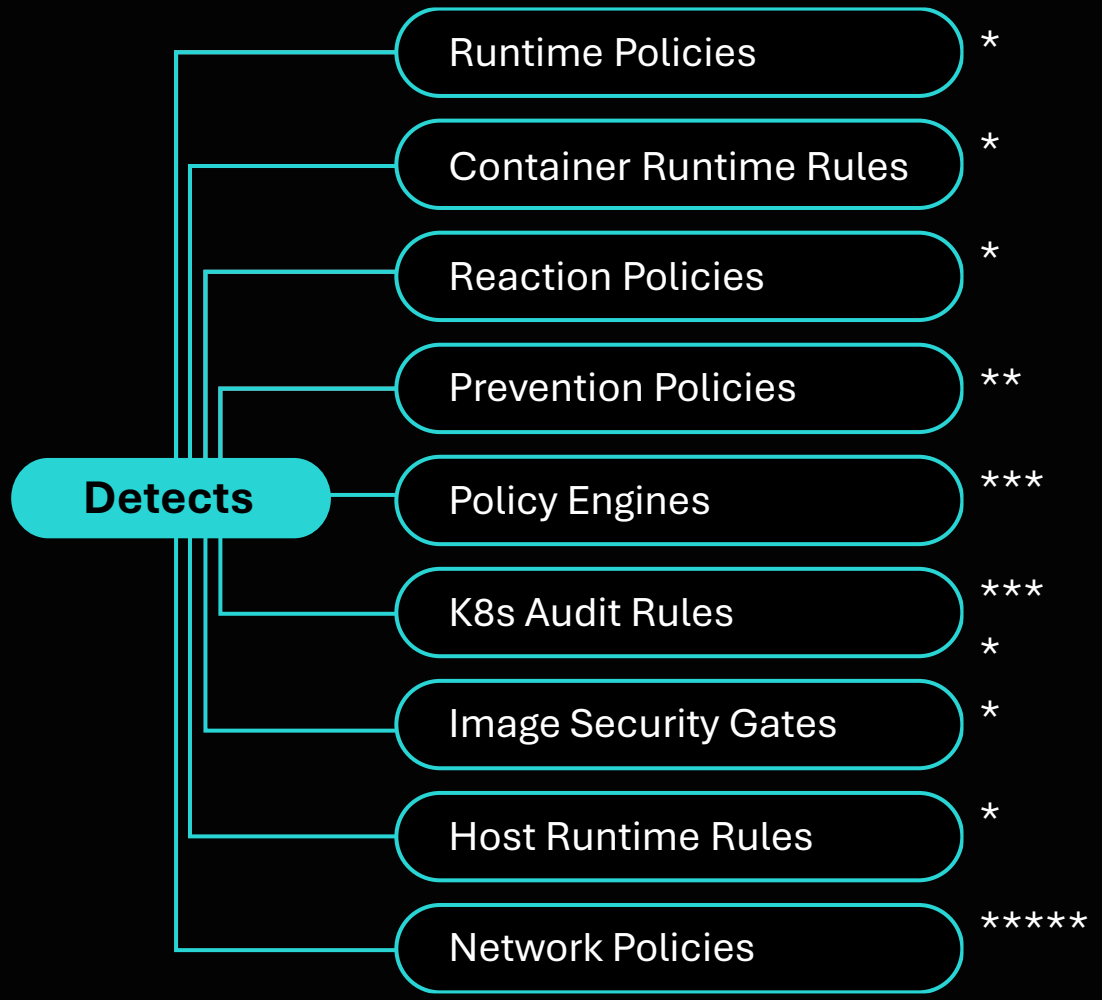
- Логи OS
- Дамп RAM память
- Дамп ФС (диск)

- Дамп RAM память
- Дамп ФС
- Runtime события

- Логи приложения

LUNTRY

Как выглядит в целом мониторинг K8s



Идеальная картина, к которой стоит стремиться, чтобы не иметь слепых зон в инфраструктуре

* - только навесным специализированным СЗИ
** - встроенные - это seccomp, AppArmor, SeLinux
*** - Validating Admission Policy с 1.30 (stable)
**** - нужно что-то, чтобы накладывать правила
***** - нужно что-то, чтобы собирать сработки с CNI

LUNTRY

Ориентиры

Цифры

SOC FORUM 2025

ДАННЫЕ МОГУТ СИЛЬНО РАЗНИТЬСЯ — ЭТО ВСЕ ДЛЯ ОРИЕНТИРА

	Среднее количество правил	Среднее количество событий
Runtime (файловые, процессные сетевые события)	50+	500-120k EPS на ноду
Аудит OS	70+	20-500 EPS
Kubernetes Audit Log	50+	10k-20k RPS (прикладной кластер 512 Nodes)

"Подключение Kubernetes к SOC: подводные камни", SOC Forum 2025

LUNTRY

Runtime агент, EDR, AV

- AV негативно влияет на контейнеры.
- EDR не в контейнерном исполнении негативно влияет на систему.
- EDR может отлично видеть, ЧТО происходит на хосте, но не видит КТО, КАК и ПОЧЕМУ это разрешено в Kubernetes.
- EDR и Container security агент создают нагрузку друг на друга.



Antivirus software and Docker

Ask Gordon Copy Markdown View Markdown

When antivirus software scans files used by Docker, these files may be locked in a way that causes Docker commands to hang.

One way to reduce these problems is to add the Docker data directory (`/var/lib/docker` on Linux, `%ProgramData%\docker` on Windows Server, or `$HOME/Library/Containers/com.docker.docker/` on Mac) to the antivirus's exclusion list. However, this comes with the trade-off that viruses or malware in Docker images, writable layers of containers, or volumes are not detected. If you do choose to exclude Docker's data directory from background virus scanning, you may want to schedule a recurring task that stops Docker, scans the data directory, and restarts Docker.

Безопасность Kubernetes – это больше, чем наблюдение за происходящим на хосте.

Обработка runtime событий

LUNTRY

Client-side-логика

- Логика идентификации нежелательного действия находится на конечной точке
- С ростом числа правил растет время и количество ресурсов, требуемых на обработку
- Доступна атакующему

Server-side-логика

- Логика идентификации нежелательного действия находится на удаленной точке
- С ростом числа правил не возрастает нагрузка на хост
- Не доступна атакующему

Политика для Audit Log

ПОЛИТИКУ МОЖНО РАЗБИТЬ НА 3 БЛОКА:

1. Детализируем важное
2. Исключаем лишнее
3. Остальное в общем режиме

```yaml
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
  - "RequestReceived"
rules:
  - level: RequestResponse
    resources:
    - group: ""
      resources: ["pods"]
  ...
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: ""
        resources: ["endpoints", "services", "services/status"]
  ...
  - level: Metadate
```

Высокий уровень детализации
Отказ от логирования
Все остальное

LUNTRY

Выводы

01 EDR подходы не работают в Kubernetes

02 Kubernetes Audit Log должен обрабатываться до попадания в SIEM

03 Cloud-native окружения требуют cloud-native подходов

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Спасибо за внимание!

Вопросы?

Дмитрий Евдокимов

de@luntry.ru

Qu3b3c

k8security