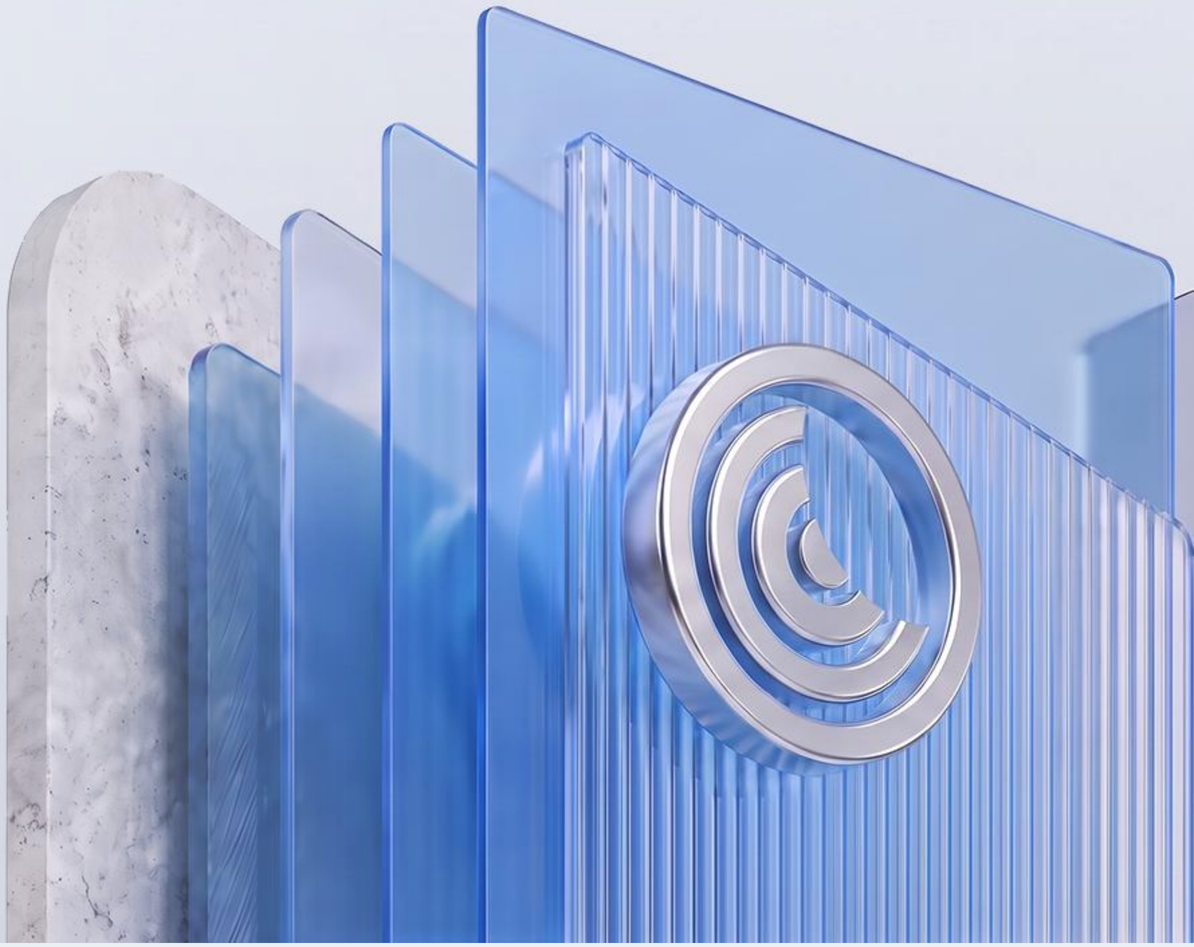
SOC FORUM 2026

Дмитрий Евдокимов

Основатель и технический директор Luntry

Реагирование на инциденты в Kubernetes для SOC



Обо мне

SOC FORUM 2026

> Я не верю в то, что систему можно сделать надежной и безопасной, не понимая того, как она устроена.



ДМИТРИЙ ЕВДОКИМОВ

Основатель
и технический директор Luntry

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

ВЫСТУПЛЕНИЯ НА КОНФЕРЕНЦИЯХ

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

Содержание презентации

SOC FORUM 2026



01 Введение

02 Особенности мониторинга и обнаружения инцидентов в Kubernetes

03 Организация процесса реагирования на инциденты в Kubernetes

04 Практические рекомендации и лучшие практики

05 Выводы

01

ВВЕДЕНИЕ



Текущая картина

SOC FORUM 2026

01

Современная разработка ПО практически полностью завязана на образах контейнеров

02

Kubernetes (K8s) безоговорочно является стандартом де-факто в области оркестрации контейнеров

03

AI открыл новые возможности по поиску уязвимостей в ПО, анализу патчей, написанию эксплоитов, автоматизации атак

04

Рои AI-агентов способны шумно (или нет), но очень быстро продвигаться по инфраструктуре жертвы

02

ОСОБЕННОСТИ МОНИТОРИНГА И ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ В KUBERNETES



Специфика контейнерных окружений

SOC FORUM 2026

01

МАЛЫЙ СРОК ЖИЗНИ КОНТЕЙНЕРОВ

03

МНОЖЕСТВО УРОВНЕЙ АБСТРАКЦИЙ

02

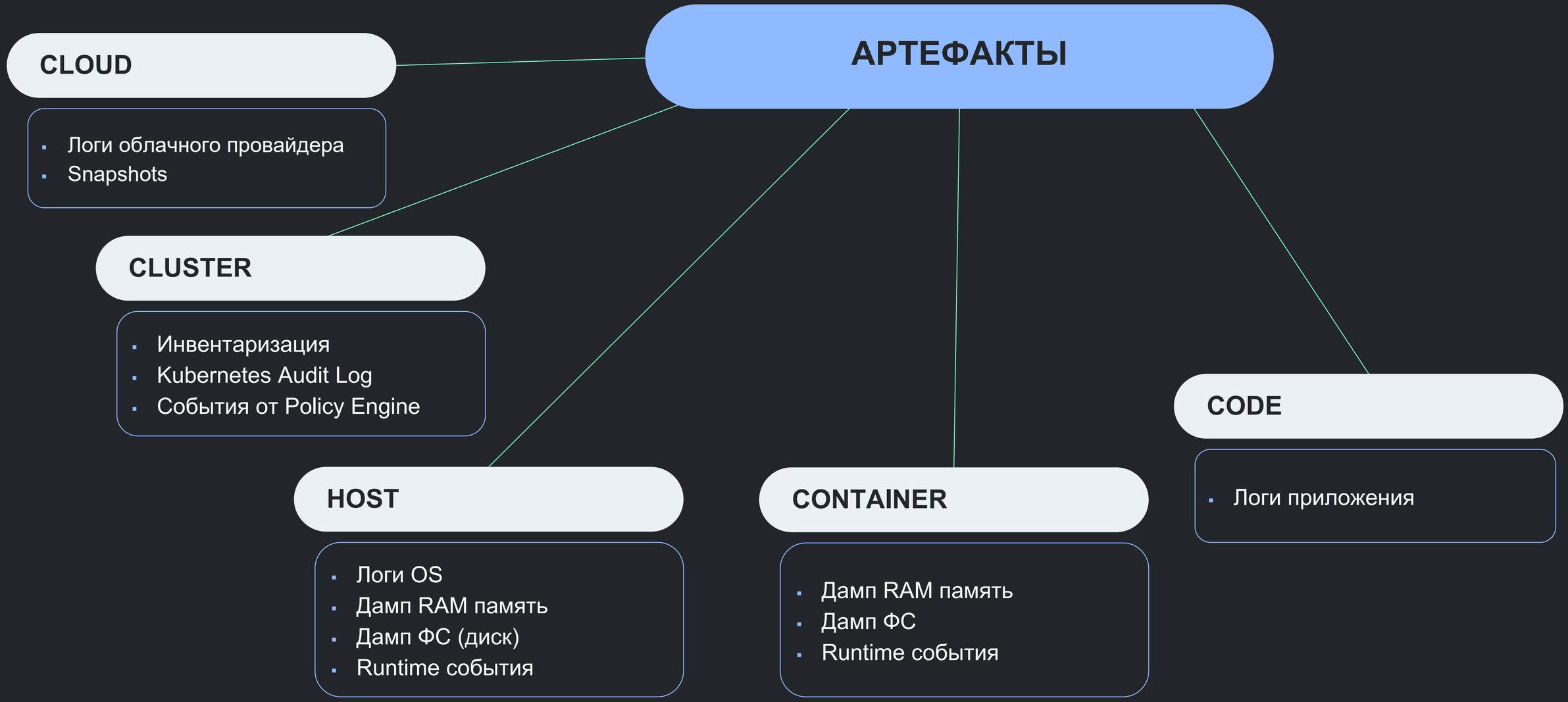
K8S: SELF-HEALING, SELF-CONTROL

04

СЛЕДЫ ЗЛОУМЫШЛЕННИКА В КОНТЕЙНЕРЕ ПРОПАДАЮТ САМИ

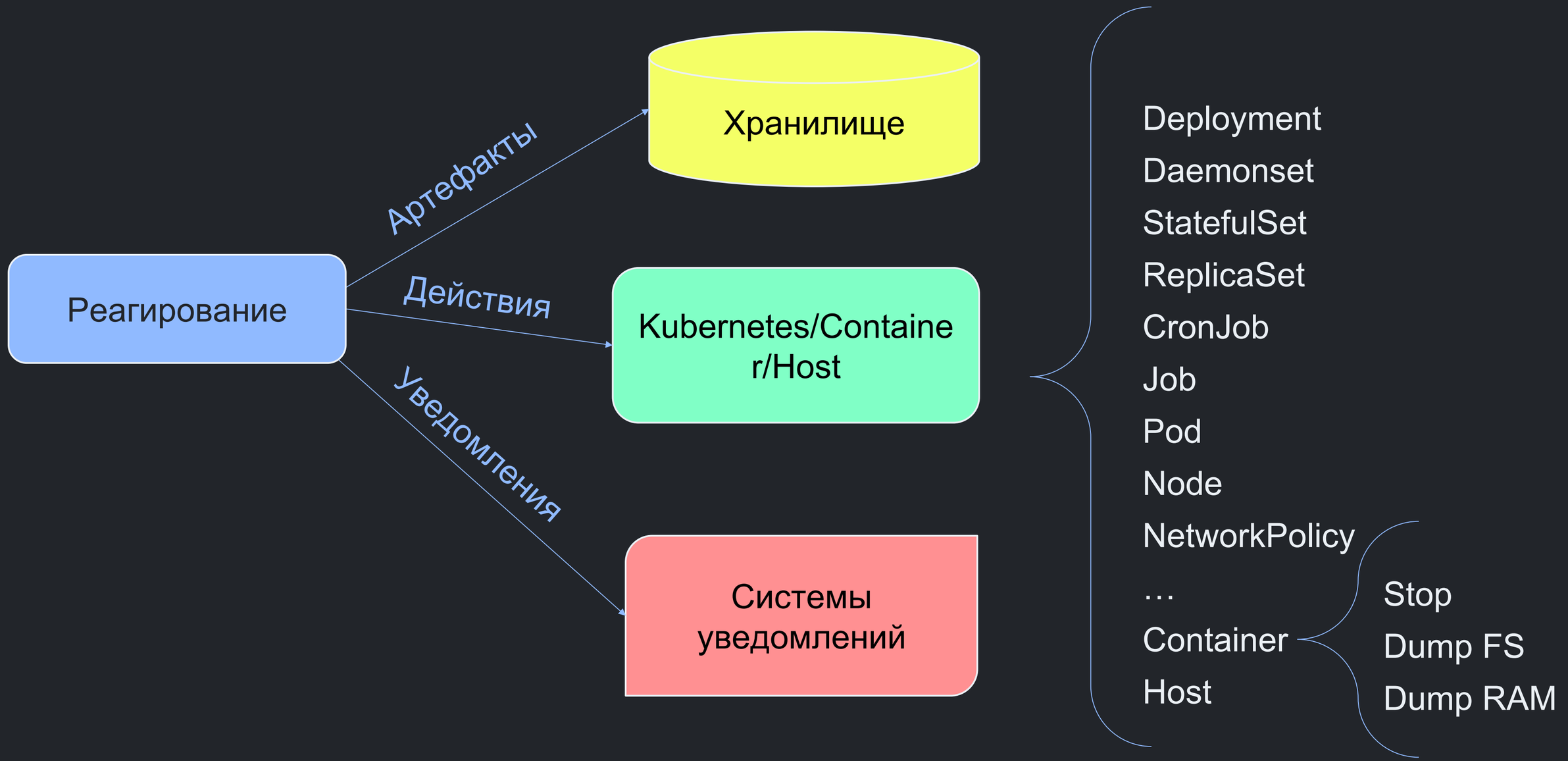
Что можно / нужно собирать с K8s окружений

SOC FORUM 2026



Основные элементы реагирования

SOC FORUM 2026



03

ОРГАНИЗАЦИЯ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В KUBERNETES



Подключение к SOC



04

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ И ЛУЧШИЕ ПРАКТИКИ



Без паники!

SOC FORUM 2026

01

Выводим Node из шедулинга

- kubectl cordon

02

Не заходим на Node или container

- Чтобы не занести ничего лишнего

03

Не завершаем,
не перезапускаем

- Чтобы не затереть артефакты и следы

04

Изолируем Pod по сети
- Deny all NetworkPolicy

05

Убеждаемся,
что побег и атаки
на рядом стоящие
сервисы невозможны

- Анализ SecurityContext
- Анализ техник не через SecurityContext

Реагирование на уровне Host

SOC FORUM 2026

УЧИТЫВАЕМ СПЕЦИФИЧНЫЕ ДИРЕКТОРИИ ОТ KUBERNETES

- Логи системных компонентов на Master и Worker Nodes (Kube-proxy, Kubelet, etcd и т.д.)
  - Так как Kubernetes — это фреймворк, расположение этих директорий может варьироваться
- Container specific OS упрощают работу
  - Можно вообще исключить модель нарушителя на Node

LINUX ХОСТ



- Актуально все, что актуально для всех Linux
- Он может быть автоматически перезагружен / отключен / обновлён / …со всеми артефактами и следами

ЛЮБАЯ ИНТЕРАКТИВНАЯ АКТИВНОСТЬ НА ХОСТЕ ЭТО СТРАННО!

Реагирование на уровне Container

ДАМП ФС КОНТЕЙНЕРА

Акцент на UpperDir

ДАМП RAM ПАМЯТИ

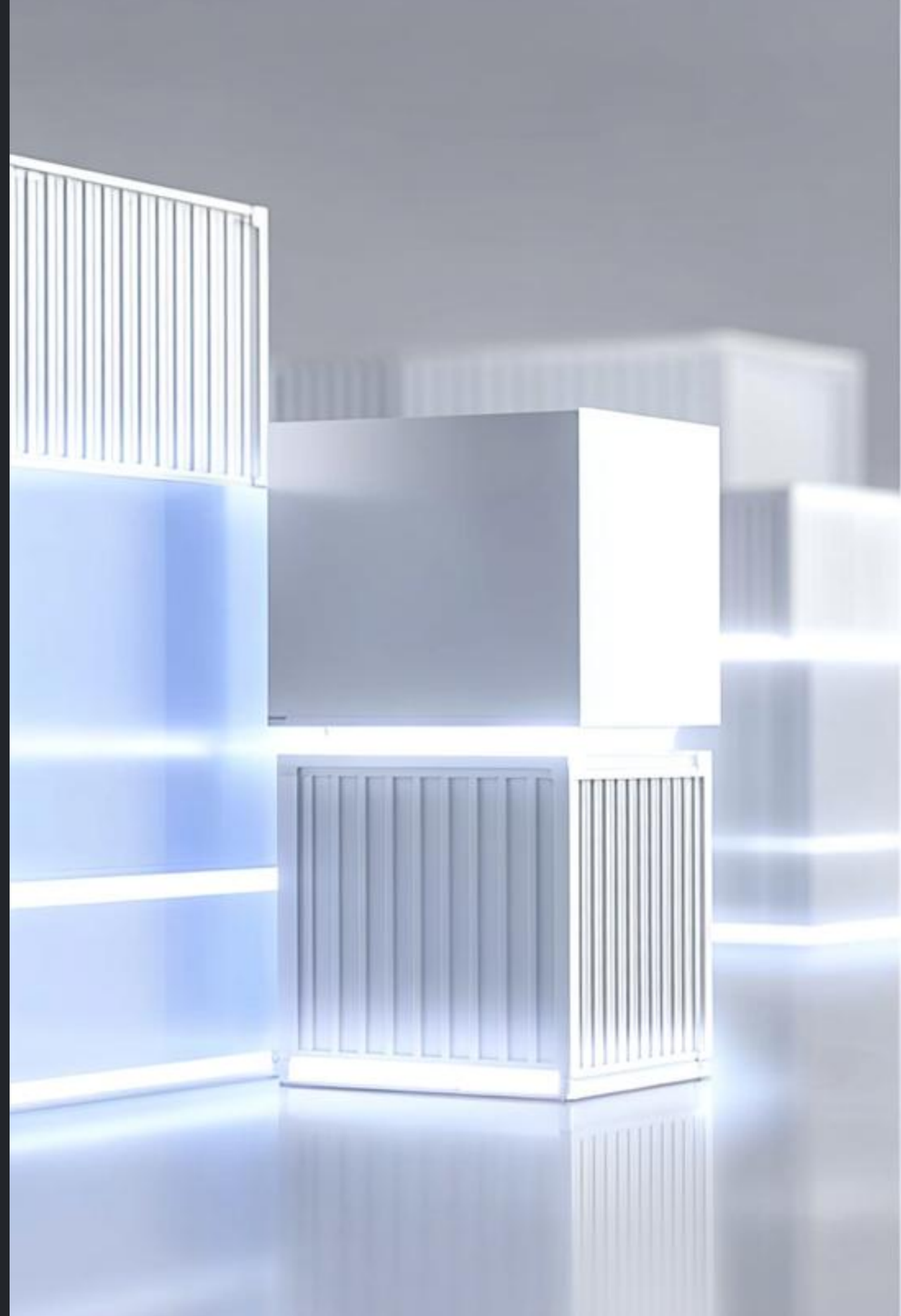
Для fileless угроз и глубокой аналитики

ОСТАНОВКА КОНТЕЙНЕРА

Завершение процесса не дает гарантий закрепления

CHECKPOINTING В K8S

Уже ближайшее будущее



Реагирование на уровне Kubernetes

SOC FORUM 2026

- Взаимодействие через Kubernetes API Server
- Работаем с Kubernetes resources и sub resources
- Реагирование на базе глаголов (verbs) по работе с ресурсами
  - Чтение
  - Создание
  - Редактирование
  - Удаление
  - Разное

Глагол	Действие
Get	Позволяет пользователю получить состояние ресурса Kubernetes.
List	Позволяет пользователю получить список ресурсов Kubernetes.
Watch	Позволяет пользователю получать уведомления об изменении состояния ресурса Kubernetes.
Create	Позволяет пользователю создать новый ресурс Kubernetes.
Update	Позволяет пользователю обновить существующий ресурс Kubernetes.
Patch	Позволяет пользователю частично обновить существующий ресурс Kubernetes.
Delete	Позволяет пользователю удалить существующий ресурс Kubernetes.
Deletecollection	Позволяет пользователю удалить коллекцию ресурсов Kubernetes.
Proxy	Позволяет пользователю обращаться к серверу API Kubernetes через прокси.
Connect	Позволяет пользователю подключаться к консоли контейнера Kubernetes.
Redirect	Позволяет пользователю перенаправлять трафик к сервису Kubernetes.
Portforward	Позволяет пользователю перенаправлять сетевой трафик к поду Kubernetes.

Операция чтение

SOC FORUM 2026

ОБОГАЩЕНИЕ КОНТЕКСТА ПЕРЕД ПРИНЯТИЕМ РЕШЕНИЯ

- Чтение манифеста Pod, для анализа его защищенности
- Определение родителя для подозрительного Pod
- Получение Node, где работает подозрительный Pod
- Проверка прав у скомпрометированного Service Account
- Анализ Events для восстановления хронологии
- Поиск контейнеров с высокой вероятность побега из него
- Анализ сетевой доступности Pod через Services, Endpoints, EndpointSlice, NetworkPolicy

ОБЩИЙ ПРОЦЕСС:

Алерт SOC → pod и workload → ServiceAccount и RBAC → node и соседние workloads → события и сетевой контекст → audit logs → решение о реагировании.

Операция создания

SOC FORUM 2026

- Создание диагностического Pod для анализа Host/Сети/…
- Создание временной RoleBinding для аварийного доступа
- Создание Kubernetes Event для фиксации действия
- Создание/модификация/удаление NetworkPolicy Native/Calico/Cilium
- Создание/модификация политик PolicyEngine (Kyverno/OPA Gatekeeper/VAP)

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  generateName: soc-quarantine-
  namespace: payments
  labels:
    created-by: soc
    incident-id: INC-2026-0042
  annotations:
    soc.example.com/expires-at: "2026-10-24T16:00:00Z"
    soc.example.com/reason: "Suspected cryptominer"
spec:
  podSelector:
    matchLabels:
      incident-target: "true"
  policyTypes:
    - Ingress
    - Egress
```

SOC создаёт только заранее определённые временные ресурсы: quarantine policy, диагностический Pod/Job, а также техническую запись о действии.

Временные ресурсы

SOC FORUM 2026

В Kubernetes нет стандартного поля expires-at, которое автоматически удалит объект. Срок действия должен контролироваться внешним процессом или playbook.

Одно из решений:
Kyverno DeletingPolicy
(бывшие Cleanup Policy)

```yaml
apiVersion: policies.kyverno.io/v1
kind: DeletingPolicy
metadata:
  name: cleanup-soc-quarantine
spec:
  schedule: "*/5 * * * *"

  matchConstraints:
    resourceRules:
      - apiGroups: ["networking.k8s.io"]
        apiVersions: ["v1"]
        resources: ["networkpolicies"]
        operations: ["*"]
        scope: Namespaced

    objectSelector:
      matchLabels:
        created-by: soc
        quarantine: "true"
        auto-cleanup: "true"

  conditions:
    - name: target-namespace
      expression: >-
        object.metadata.namespace == 'payments'

    - name: older-than-four-hours
      expression: >-
        time.now() - timestamp(object.metadata.creationTimestamp)
        > duration('4h')
```

Операция редактирования

SOC FORUM 2026

- Пометить подозрительный Pod/Node с помощью labels и / или annotations для расследования и выбора политиками
- Отключить автоматическое монтирование скомпрометированного токена ServiceAccount
- Убрать разрешения из выделенной Role

```
kubectl patch pod suspicious-pod -n payments \
--type=merge \
-p '{
  "metadata": {
    "labels": {
      "incident-target": "true",
      "incident-id": "INC-2026-0042"
    }
  }
}'
```

```
kubectl patch serviceaccount payment-api -n payments \
  --type=merge \
  -p '{"automountServiceAccountToken":false}'
```

SOC использует PATCH и UPDATE для управляемого изменения состояния: маркировки объектов, остановки запусков, ограничения размещения и сокращения полномочий.

Для каждого действия заранее определены область воздействия, условия выполнения, проверка результата и порядок восстановления.

Операция удаления

SOC FORUM 2026

- Завершение скомпрометированного Pod
- Удаление какого-либо Kubernetes ресурса
- На пример, RoleBinding\ClusterRoleBinding, ServiceAccount, Secret
- Удалить диагностические Pod

```
SELECTOR="created-by=soc,cleanup=true,incident-id=INC-2026-0042"

kubectl get pods \
  -n security-tools \
  -l "${SELECTOR}" \
  -o wide

curl --fail-with-body \
  -X DELETE \
  -G \
  "${API}/api/v1/namespaces/security-tools/pods" \
  --data-urlencode "labelSelector=${SELECTOR}"
```

При реагировании SOC может использовать delete для удаления конкретного объекта, а deletecollection — для удаления набора объектов по селектору.

Типичные сценарии: остановить вредоносную задачу, удалить временный доступ или очистить диагностические ресурсы после расследования.

Разнородные операции

SOC FORUM 2026

01

pods / exec

- Выполнить команду / скрипт внутри контейнера Pod
- Скачать файл из контейнера Pod

02

deployments / scale

- остановить скомпрометированный Deployment через scale

03

pods / ephemeralcontainers

- Запуск полностью своей логики
- На пример, запуск сетевого снифера

04

pods / log

- Получение лога от Pod

05

комплекс прав для

- kubectl cordon <node-name>
- kubectl drain <node-name>

Сложные / комбинированные сценарии

SOC FORUM 2026

Во время реакции может понадобиться на одно действие, а несколько.



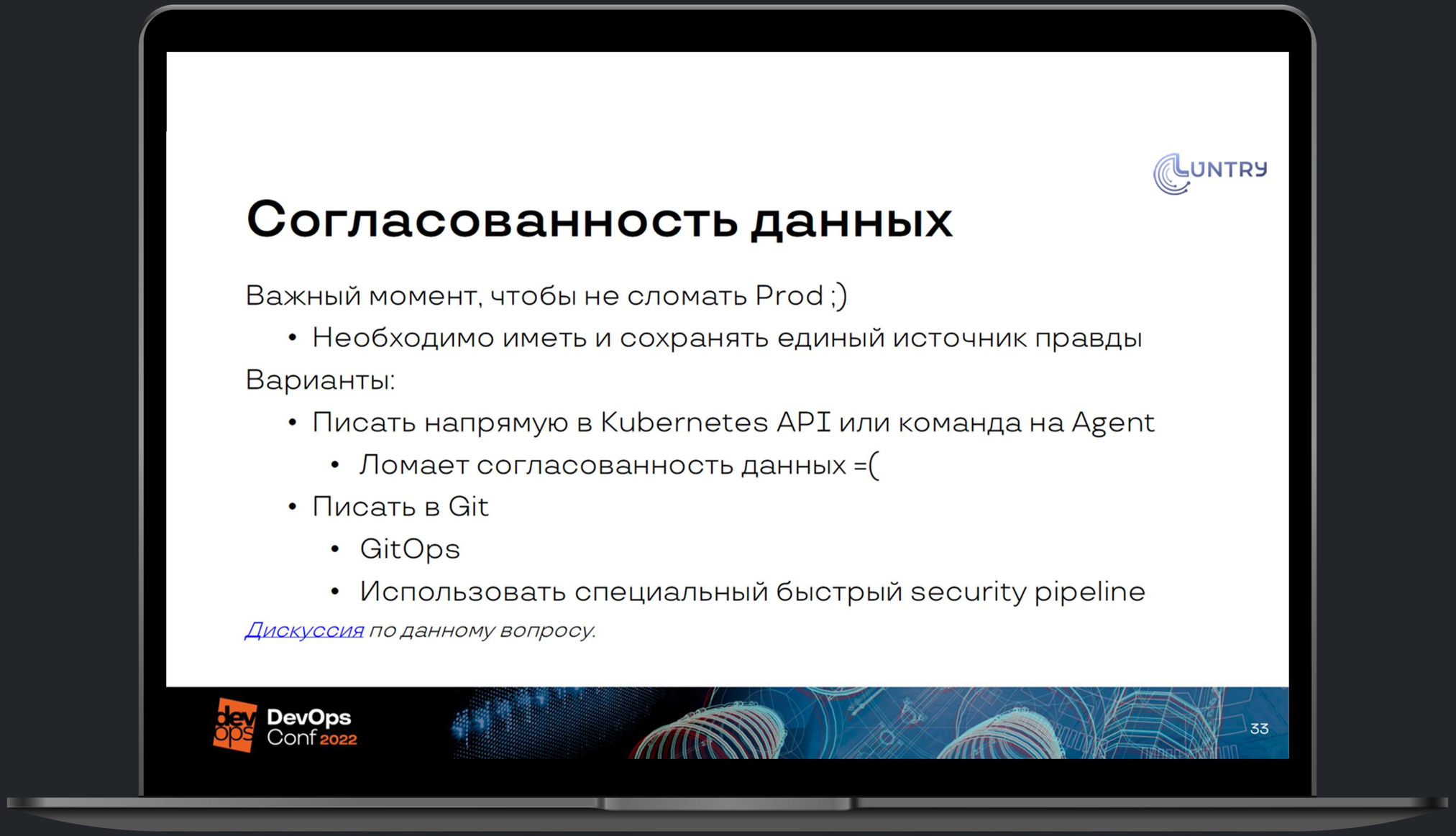
ПРИМЕР 1: ИЗОЛЯЦИЯ POD

1. Создаем изолирующую NetworkPolicy, привязывающуюся по label
2. Ставим Label на Pod, который нужно изолировать

ПРИМЕР 2: ОТЗЫВ SERVICE ACCOUNT TOKKEN

1. Создаем новый Service Account
2. Редактируем Deployment для добавления нового Service Account
3. Удаляем старый Service Account

Важно!


LUNTRY
Согласованность данных
Важный момент, чтобы не сломать Prod ;)
• Необходимо иметь и сохранять единый источник правды
Варианты:
• Писать напрямую в Kubernetes API или команда на Agent
• Ломает согласованность данных =(
• Писать в Git
• GitOps
• Использовать специальный быстрый security pipeline
Дискуссия по данному вопросу.
DevOps Conf 2022
33

05

ВЫВОДЫ



SOC
FORUM
2026

РЕАГИРОВАНИЕ В KUBERNETES — ЭТО НЕ ТОЛЬКО РАССЛЕДОВАНИЕ ВНУТРИ КОНТЕЙНЕРА.

SOC должен связать события на хосте, в контейнере и в Kubernetes API, определить границы компрометации и выбрать способ локализации, который не уничтожит доказательства и не приведёт к повторному запуску скомпрометированной нагрузки.

Полезные материалы

SOC FORUM 2026

01	«Подключение Kubernetes к SOC: подводные камни», SOC Forum 2025
02	«Безопасность контейнеров и Kubernetes для SOC», Вебинар Luntry
03	«Форензика для контейнеров и контейнерных инфраструктур», CyberCamp 2025
04	«Kubernetes Audit Log в арсенале SOC», SOC Forum 2024
05	«SOC в контейнерах», SOC Forum 2023
06	«EDR vs Containers: актуальные проблемы», SOC Forum 2023
07	«SOAR в Kubernetes малой кровью», DevOpsConf 2022
08	«Расследование инцидентов в средах контейнеризации», CyberCamp 2022



SOC FORUM 2026

Luntry.ru

luntry_official

luntrysolution

luntrysolution

info@luntry.ru

СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Евдокимов,
Основатель & Технический директор

de@luntry.ru

Qu3b3c

k8security