SOC FORUM 2025

Подключение Kubernetes к SOC: подводные камни

20.11

МОСКВА

ДМИТРИЙ ЕВДОКИМОВ

Luntry
Основатель и Технический директор

МАКСИМ ЖЕВНЕРЕВ

ГК «Солар»
Руководитель направления технологического развития JSOC

О нас

SOC FORUM 2025

Дмитрий Евдокимов

Специализация — безопасность контейнеров и Kubernetes

Максим Жевнерев

Специализация — мониторинг и реагирование на инциденты

План доклада

SOC FORUM 2025

01 **Введение**

02 **Стадии**

a. Планирование

b. Подключение и настройка

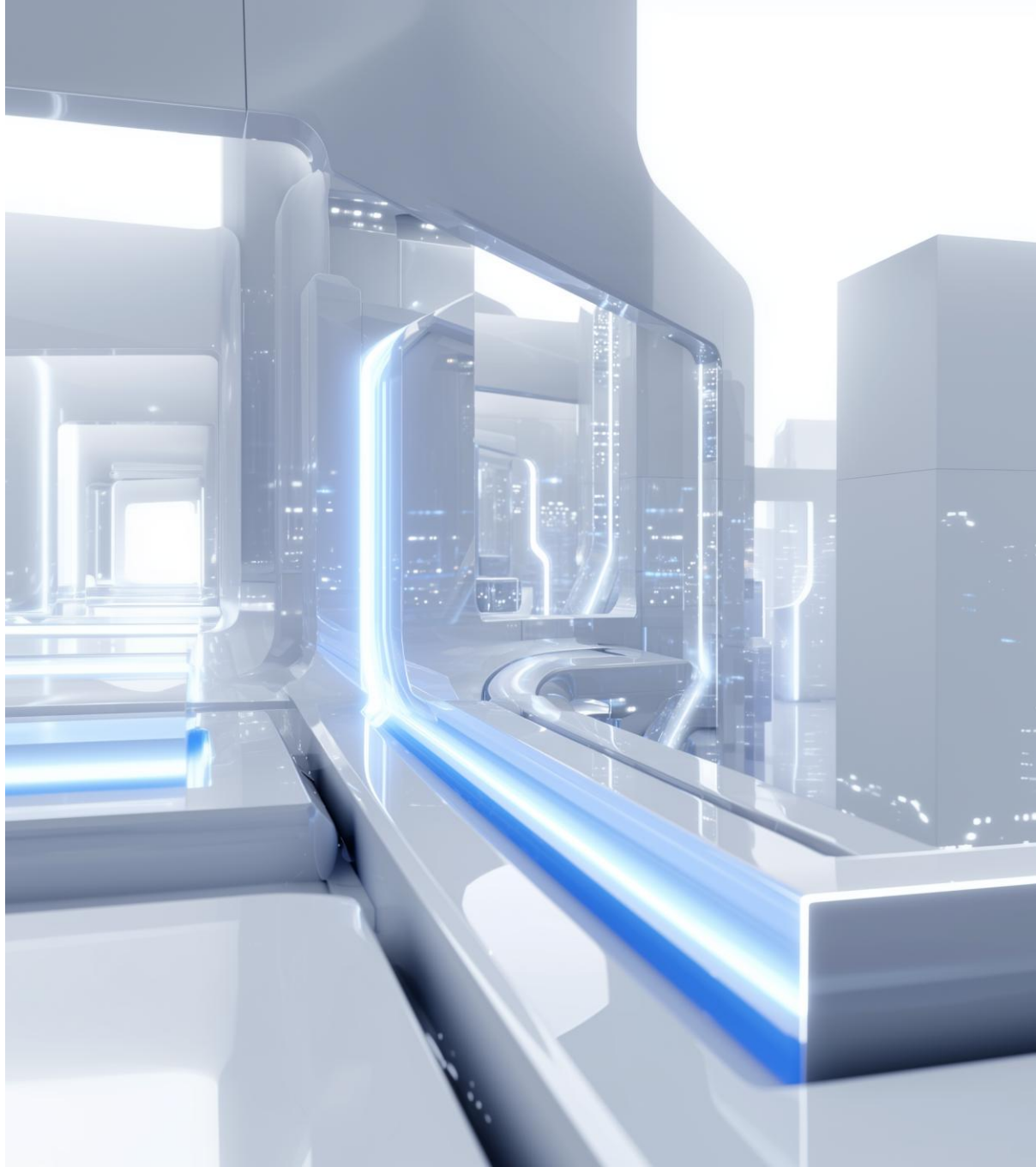
c. Мониторинг и расследование

d. Реагирование

03 **Выводы**

01

ВВЕДЕНИЕ



PPT

SOC FORUM 2025

ЛЮДИ (PEOPLE)

- L1, L2, L3
- Внутренний или внешний SOC
  - Поиск и обучение людей
- За рамками данного выступления

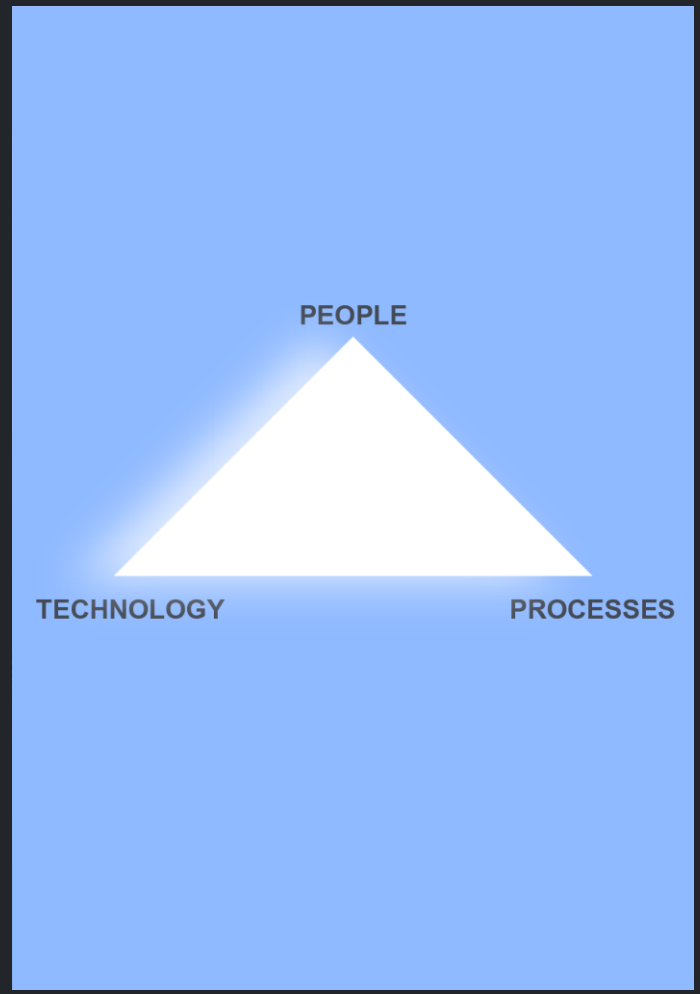
ПРОЦЕССЫ (PROCESS)

- Рассмотрим в рамках данного выступления

ТЕХНОЛОГИИ (TECHNOLOGY)

- Рассмотрим в рамках данного выступления

It is critical to note that without perpetual education and training on use and integration of these concepts, tools, and processes, adoption and application will not persist and may revert.



В чем особенности Kubernetes?

SOC FORUM 2025

PaaS

- Еще один уровень надстройки
  - Не отменяет работы на нижележащих уровнях
- Эфемерная инфраструктура
  - Динамическое окружение
  - Малый срок жизни контейнера
- Высокая нагрузка
  - Большое количество событий и данных
- Бизнес система
  - Все окружения уникальны

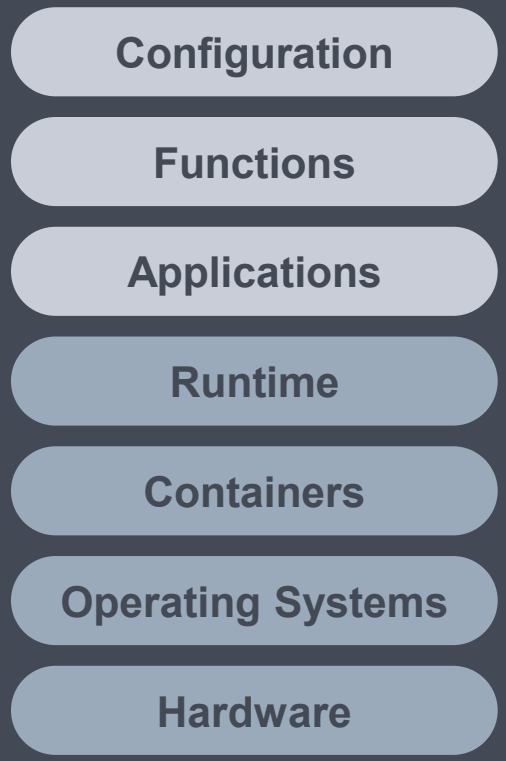
Декларативная система

- Все YAML
- Множество уровней абстракций

Саморегулируемая система

- Self-healing, self-control, Control loop, reconciliation loop

Platform as a service (Paas)

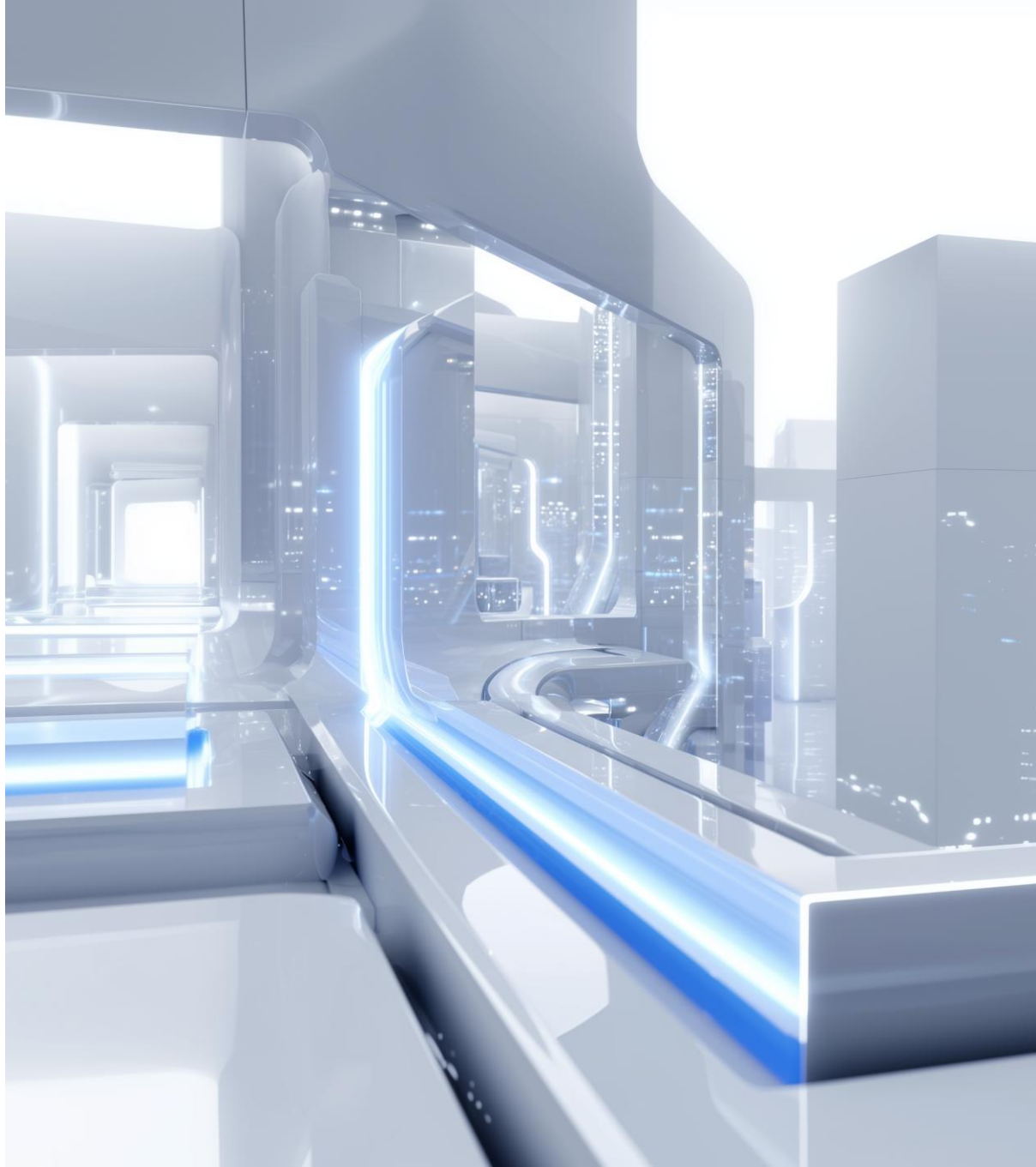


Что такое «подключить к SOC»?

SOC FORUM 2025

02

СТАДИЯ ПЛАНИРОВАНИЯ



Кто отвечает за безопасность Kubernetes?

SOC FORUM 2025

«Почему защитой k8s должно заниматься целое подразделение?», Артем Мерец, (Т-Банк), БеКон 2024

Как Kubernetes живет в инфраструктуре?

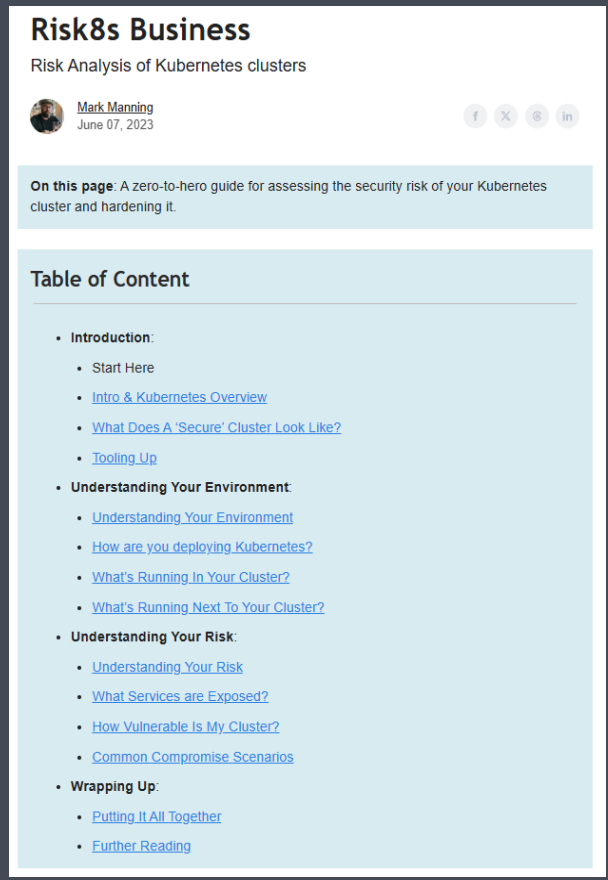
SOC FORUM 2025

ЧАСТЬ 1:

- Где находятся кластера?
- Насколько большие кластера?
- Как развернут Kubernetes кластер?
- Что запущено в кластере?
- Что работает рядом с кластером?

ЧАСТЬ 2:

- Кто может работать с кластером?
- Как сервисы запускают в кластере?
- Какие сервисы смотрят наружу?
- Какие сервисы доступны внутри?
- Насколько кластер просматриваемый (visibility, observability)?
- Насколько кластер уязвим?



Risk8s Business

Risk Analysis of Kubernetes clusters

Mark Manning
June 07, 2023

On this page: A zero-to-hero guide for assessing the security risk of your Kubernetes cluster and hardening it.

Table of Content

- **Introduction**:
  - Start Here
  - Intro & Kubernetes Overview
  - What Does A 'Secure' Cluster Look Like?
  - Tooling Up
- **Understanding Your Environment**:
  - Understanding Your Environment
  - How are you deploying Kubernetes?
  - What's Running In Your Cluster?
  - What's Running Next To Your Cluster?
- **Understanding Your Risk**:
  - Understanding Your Risk
  - What Services are Exposed?
  - How Vulnerable Is My Cluster?
  - Common Compromise Scenarios
- **Wrapping Up**:
  - Putting It All Together
  - Further Reading

Risk8s Business

Какие активности хотим отслеживать?

SOC FORUM 2025

1. Общие вопросы \ базовая «гигиена»
   - Кто работает с системой, откуда могут подключаться?
   - Как устроена ролевая модель?
   - Где критичные данные и кто может иметь к ним доступ?

2. Сценарии атак \ угрозы
   - Общее описание процесса работы в системе
   - Какие ограничения в процессах есть?
   - Каких их можно по мнению владельца обойти?
   - **Проводите pentest \ red team для выявления слабых мест**

3. Как устроены основные бизнес-процессы

«Экскурсия по матрицам угроз для контейнеров и Kubernetes», Сергей Канибор (Luntry), VK Kubernetes Conf 2023

«Kubernetes Audit Log в арсенале SOC», Дмитрий Евдокимов (Luntry), SOC Forum 2024

Какие данные и откуда мы можем получить?

SOC FORUM 2025

01

Есть ли внутренний аудит лог?

Для каких компонент?

02

Есть ли какая-либо инвентаризационная информация, как можно использовать?

03

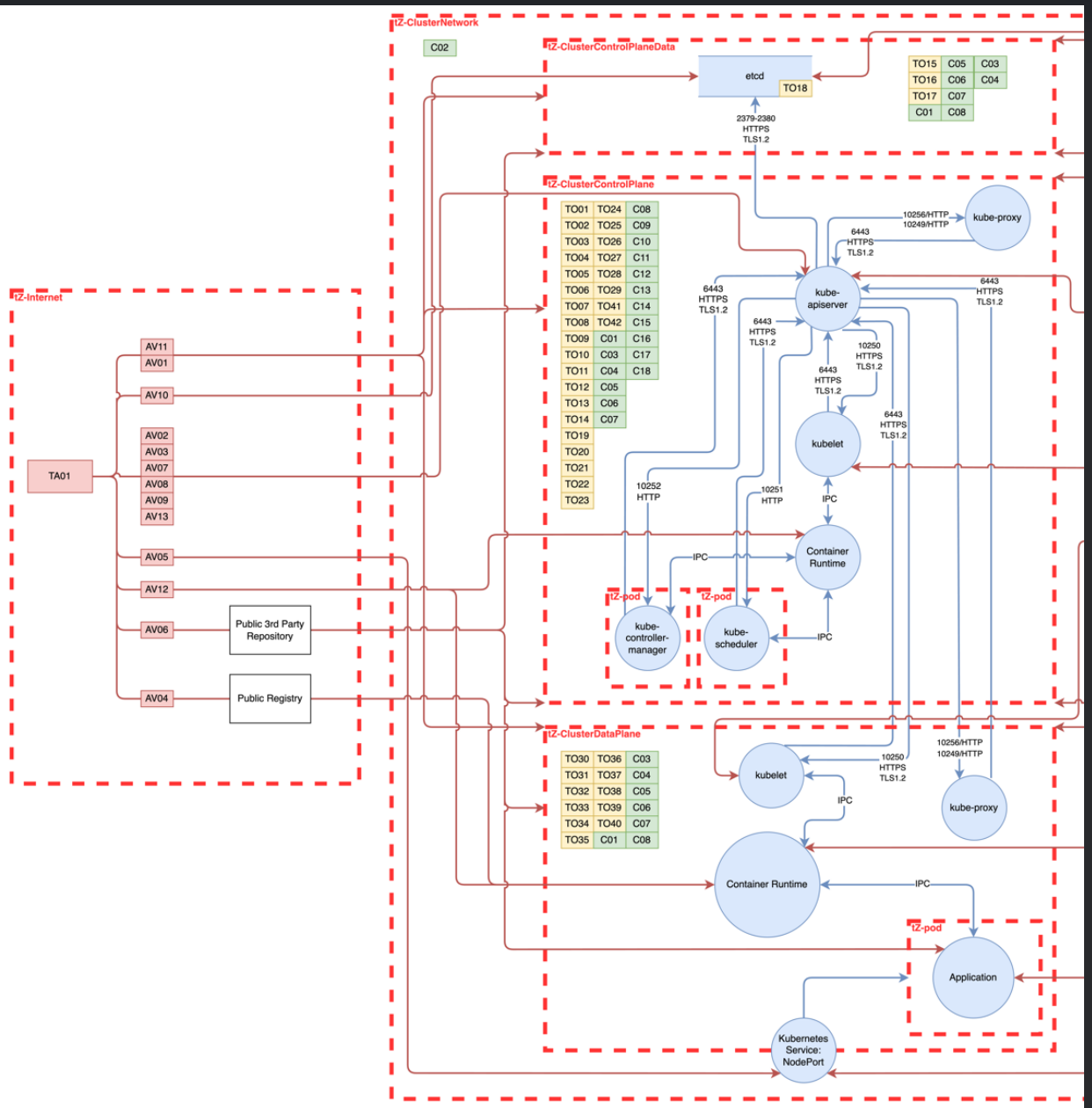
Есть ли «навесные» \ встроенные средства защиты?

Источники

Attack Vectors (AV)	
ID	**Description**
AV01	Publicly exposed host with vulnerable non-K8s endpoint(s)/service(s)/port(s).
AV02	Compromised kubeconfig file.
AV03	Compromised K8s service account token with cluster details.
AV04	Malicious container image in public registry.
AV05	Publicly exposed vulnerable K8s workload: e.g. RCE.
AV06	Malicious 3rd party dependency.
AV07	kube-apiserver vulnerability.
AV08	kube-apiserver's options configured incorrectly.
AV09	kube-apiserver's authorization configured incorrectly.
AV10	etcd's authentication configured incorrectly.
AV11	Compromised credentials of publicly exposed host.
AV12	Container runtime configured incorrectly.
AV13	Compromised OIDC token with cluster details.
AV14	Host with vulnerable non-K8s endpoint(s)/service(s)/port(s).
AV15	Legitimately obtained kubeconfig file.
AV16	Legitimately obtained K8s service account token with cluster details.
AV17	Malicious container image in private registry.
AV18	Vulnerable K8s workload: e.g. RCE.
AV19	kubelet vulnerability.
AV20	kubelet's options configured incorrectly.
AV21	Compromised credentials of host.
AV22	Legitimately obtained OIDC token with cluster details.
AV22	Legitimately obtained credentials of host.

Assumptions (AS)	
ID	**Description**
AS01	Fault-tolerance and high availability are not in scope for this model
AS02	Two certificate authorities (CAs) are in scope for this model: one for the cluster and one for etcd.
AS03	Within this model, the kube-proxy is running as a service in the host and using a config file.
AS04	Container Runtime installation and related files are out of scope for this model.
AS05	Within this model, there are no business-type K8s workloads scheduled in the master node.
AS06	Within this model, K8s admission controllers include: ResourceQuota, LimitRanger, PodSecurity(Policy), and ImagePolicyWebhook.
AS07	Within this model, K8s authorisation is limited to: RBAC, Node, and Webhook.
AS08	Within this model, K8s encryption is implemented via EncryptionConfiguration and applies for data at rest only.
AS09	Within this model, K8s MutatingAdmissionController enables: disable service account token auto-mount, PodSecurityContext/ContainerSecurityContext, AppArmor, container sandboxing, and application logging consumption.
AS10	Within this model, K8s authentication is limited to: client certificates, service account tokens, and OIDC tokens.
AS11	AV02, AV03, AV07, AV08, AV09, AV10, AV12, and AV13 are being taken into account under the assumption that the hosts holding the cluster control plane's components are publicly exposing them.

Controls	
ID	**Description**
C01	C-Harden-Component
C02	C-Control-Traffic-Flow
C03	C-Harden-Config-Compl-Mon / C-Mon-Drift
C04	C-Evt-Log-App / C-Evt-Log-Sec / C-Evt-Log-Sys
C05	C-Mon-File-Integrity
C06	C-Mon-Log
C07	C-Mon-Health
C08	C-Vuln-Scan
C09	C-K8s-Harden-Component
C10	C-K8s-AdmissionControllers
C11	C-K8s-AuditLogs
C12	C-K8s-Authorisation
C13	C-K8s-CNI-NetworkPolicies

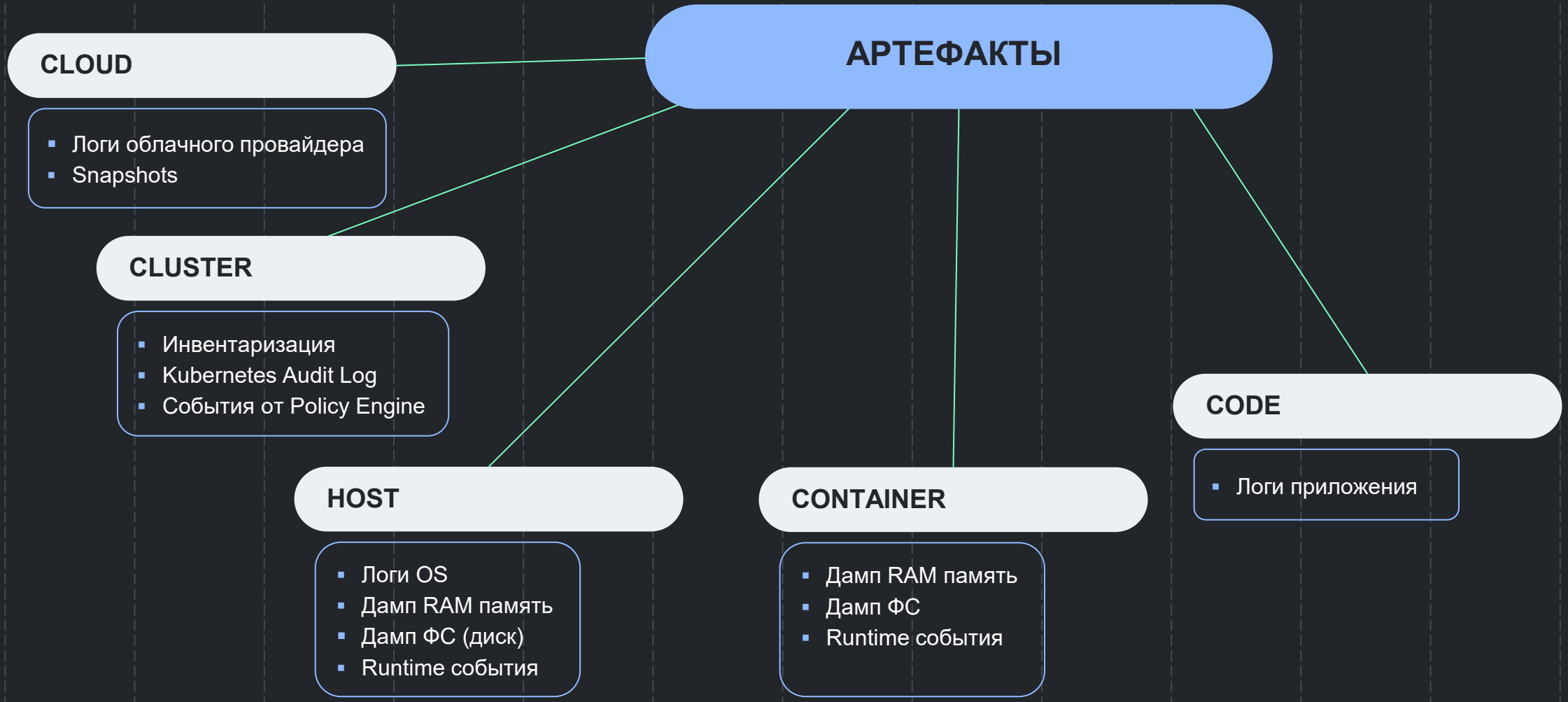


SOC FORUM 2025

[kubernetes-for-soc]

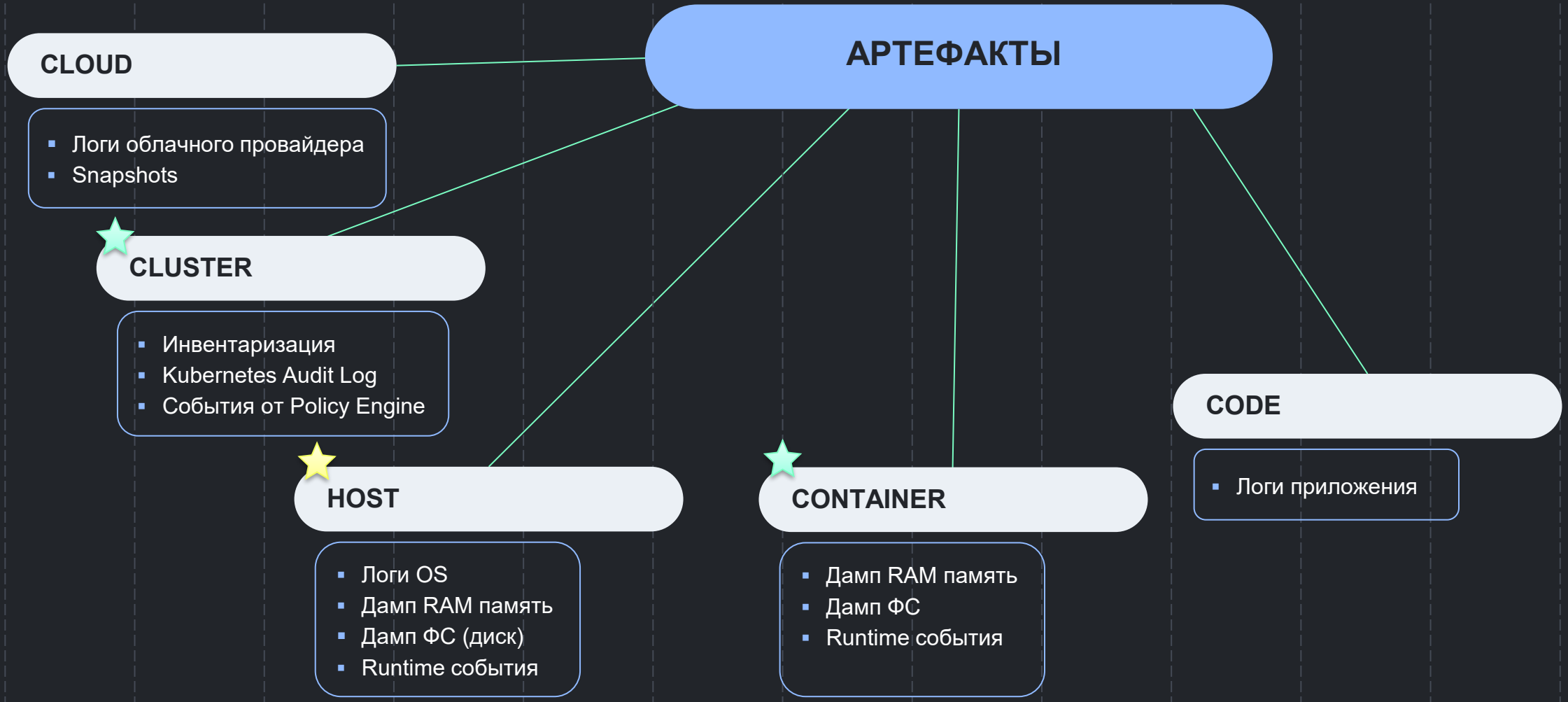
Что можно собирать с K8s окружений

SOC FORUM 2025



Что можно собирать с K8s окружений

SOC FORUM 2025



Уровень Cluster

SOC FORUM 2025

ИНВЕНТАРИЗАЦИЯ

- Данные с Kubernetes API Server
- Подписка на обновление / изменение k8s ресурсов

СОБЫТИЯ ОТ POLICY ENGINE

- Нужно использовать Kyverno, OPA Gatekeeper, VAP
- Политики могут работать в audit и enforce режимах
- Изучаем, как и любые другие логи

KUBERNETES AUDIT LOG

- По умолчанию выключен
- Нужно заранее корректно настроить Audit Policy
- Изучаем, как и любые другие логи

Уровень Host

SOC FORUM 2025

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!

Уровень Container

Классический Linux Container

Linux process + cgroup + namespaces (pid, user, uts, ipc, net, mnt, …) + pivot_root + image

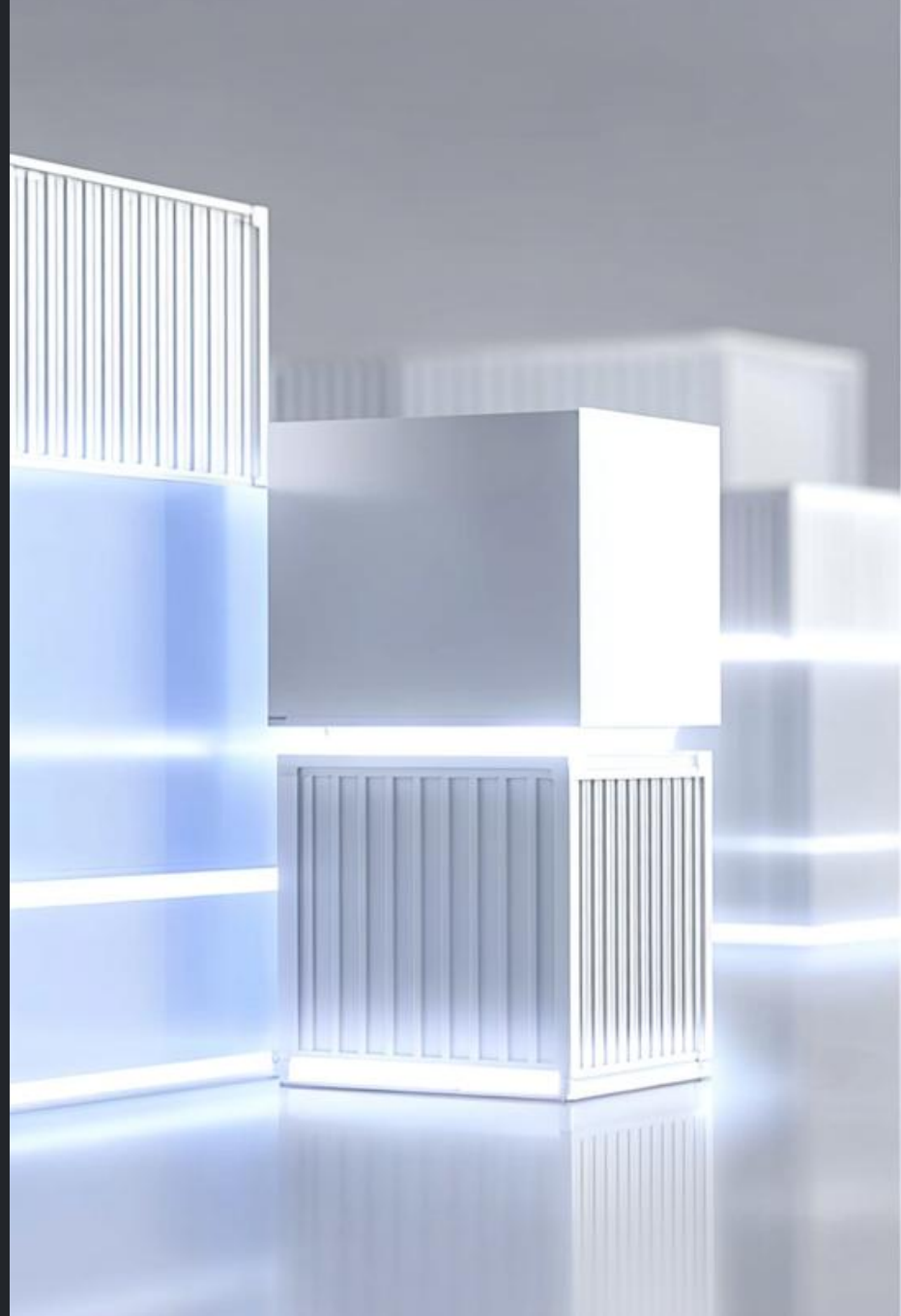
Контроль Runtime событий

Файловые, сетевые, процессные события

Container Image

Неизменяемый пакет файлов операционной системы, кода приложения и любых зависимостей приложения. OverlayFS.

Контроль запуска только разрешенных images



Ресурсы (железо)

SOC FORUM 2025

Заранее нужно планировать

- Runtime сенсоры кушают ресурсы на каждой ноде
- Kubernetes Audit Log ест ресурсы на Master Nodes

Привет HighLoad!

- Сильное отличие от пользовательских рабочих станций
- Плавающая нагрузка

Как в процессе сбора, обработки информации, так и при ее хранении

- CPU
  - Никто не хочет замедлять свои микросервисы
  - Никто не хочет отдавать много процессорных ядер под агенты на Nodes
- Memory
  - Агенты генерируют большой объем данных

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)

Выводы по разделу

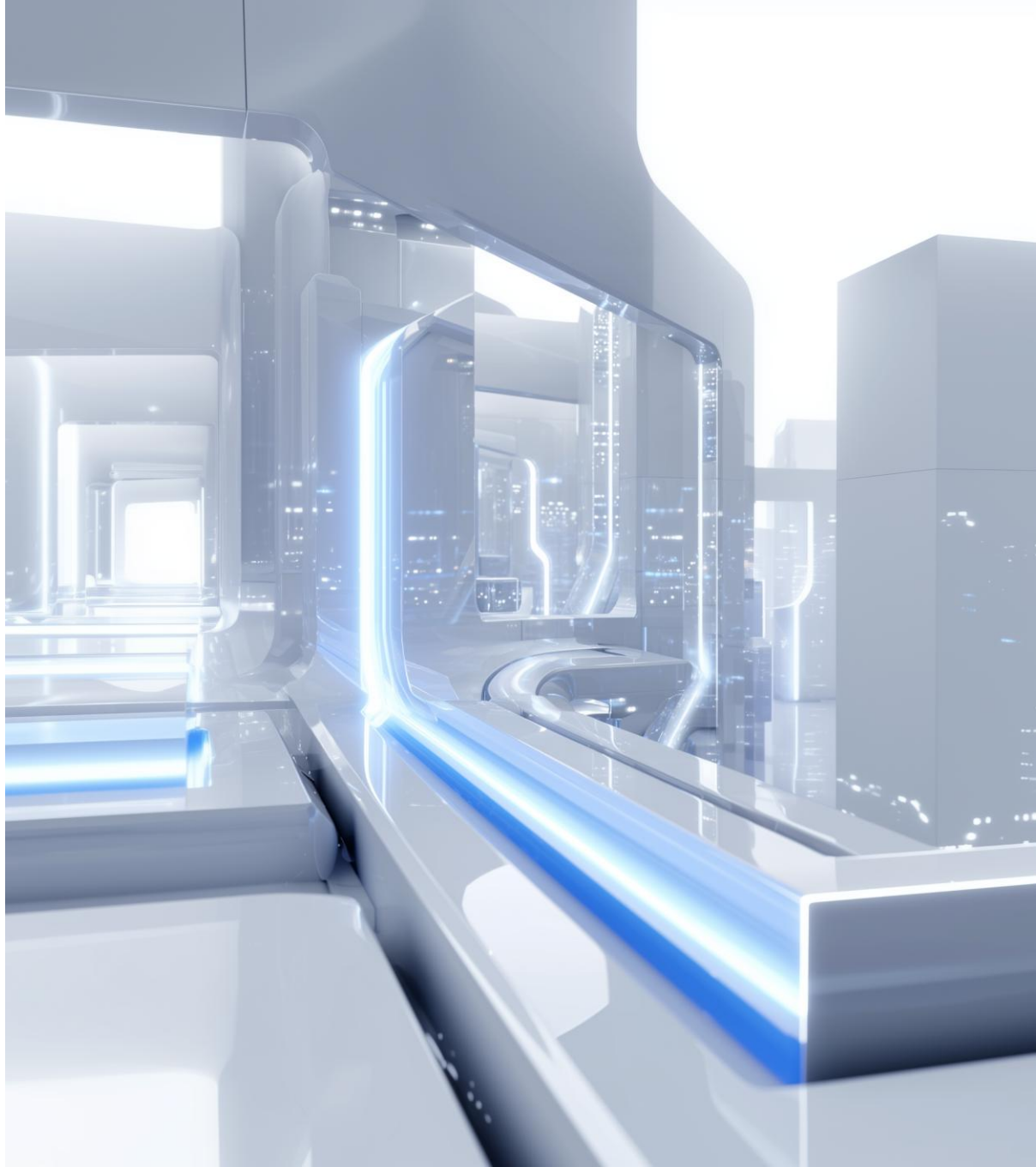
SOC FORUM 2025

- **Kubernetes** — дополнительный слой абстракции, который добавляет еще дополнительных требований к мониторингу к тому объему, что уже делается (или должны делать :))

- **Планирование** – важный этап, который сэкономит много сил и нервов при дальнейшей настройке

03

СТАДИЯ ПОДКЛЮЧЕНИЯ И НАСТРОЙКИ



Как происходит процесс подключения?

SOC FORUM 2025

Поиск необходимых событий

Если в логе нет событий — это не означает, что их нельзя воспроизвести

Выбор транспорта для сбора

Выбираем тот, где для нужных событий будет больше информации

Разработка сценариев

Типовые сценарии мониторинга + специфика под бизнес-кейс.

Анализ полноты событий

Важно понимать,
что в событиях есть нужный набор данных

Разработка парсеров

Стараемся забирать данные в «готовом» формате.

Как происходит процесс подключения?

SOC FORUM 2025

Поиск необходимых событий

Если в логе нет событий — это не означает, что их нельзя воспроизвести

Выбор транспорта для сбора

Выбираем тот, где для нужных событий будет больше информации

Разработка сценариев

Типовые сценарии мониторинга + специфика под бизнес-кейс.

Анализ полноты событий

Важно понимать,
что в событиях есть нужный набор данных

Разработка парсеров

Стараемся забирать данные в «готовом» формате.

Какие типы событий как правило ищем?

SOC FORUM 2025

01

Можно ориентироваться на ГОСТ 59548-2022

02

Для различных категорий систем характерны определенные типы событий

03

Базовый минимум:

a. Аутентификация
b. Управление пользователями \ привилегиями
c. Выполнение команд
d. Изменение конфигурации

Пример: поищем аутентификацию в Kubernetes?

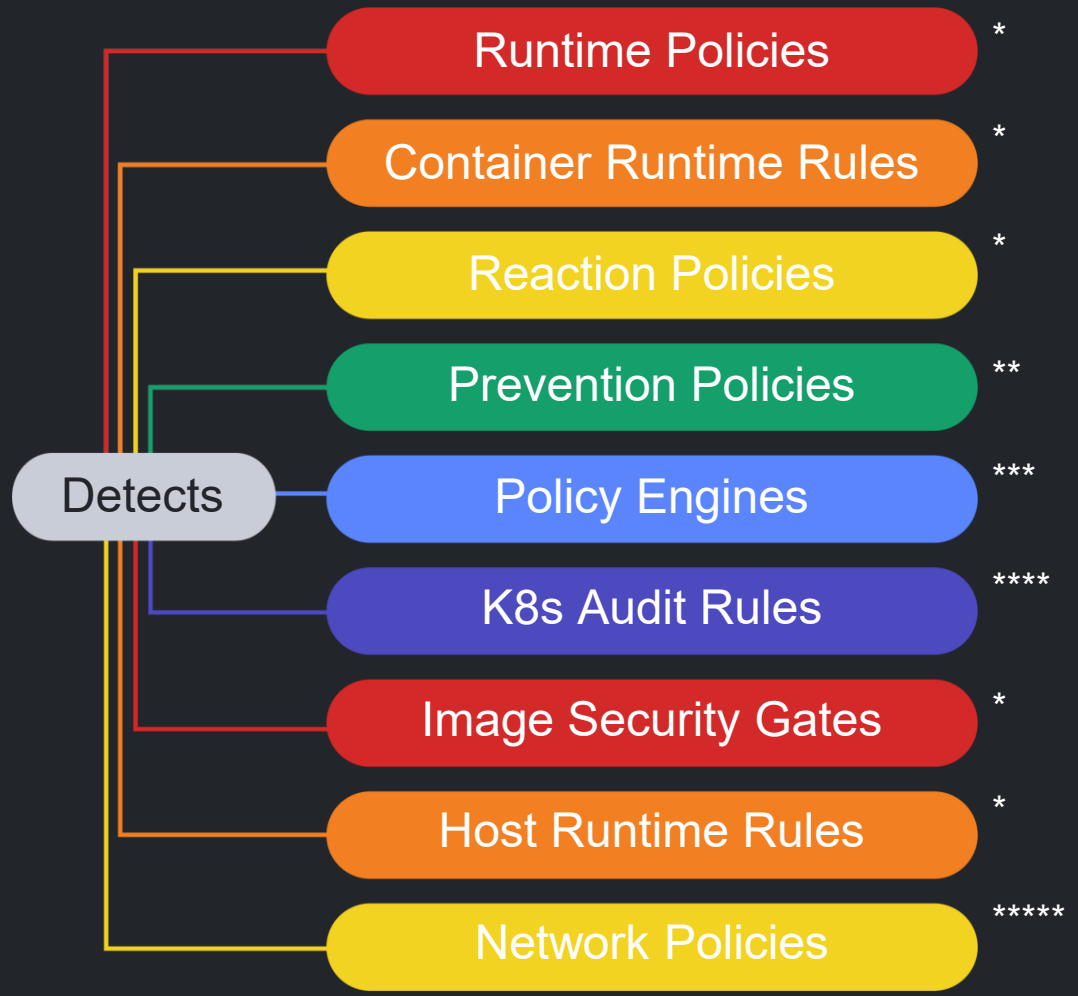
SOC FORUM 2025

- В Audit Log **нет события** аутентификации.
- “Голый” Kubernetes - обычно не используют, события можно брать из внешних систем
- Как правило аутентификация через внешние провайдеры (OpenID Connect)

keycloak_1 | 16:42:11,284 WARN [org.keycloak.events] (default task-5)
type=LOGIN_ERROR,
realmId=prod,
clientId=kubernetes,
userId=3f29b1a2-4baf-4c6d-9e92-e3a4d3dd8f91,
ipAddress=10.32.15.7,
error=invalid_user_credentials,
auth_method=openid-connect,
auth_type=code,
redirect_uri=https://k8s-api.example.com:6443/oauth2/idpresponse,
code_id=8c31d28f-5521-4f4c-bf17-932d9a38e1a3,
username=devops-user,
authSessionParentId=7f1e7ebd-2fb8-4d94-b4a0-7494d1c24c0b,
authSessionTabId=Yt9QpZbP0sM

Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025

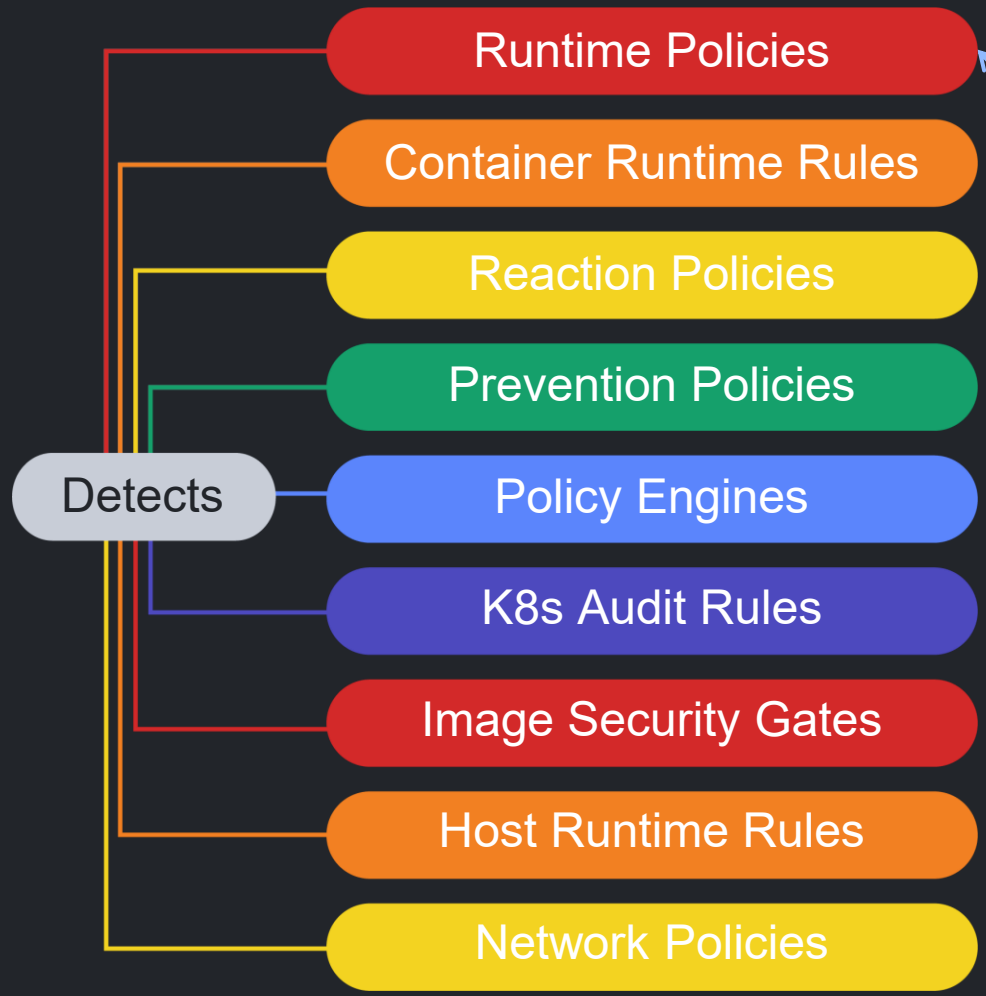


Идеальная картина к которой стоит стремиться, чтобы не иметь слепых зон в инфраструктуре

* - 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

Как выглядит в целом мониторинг Kubernetes

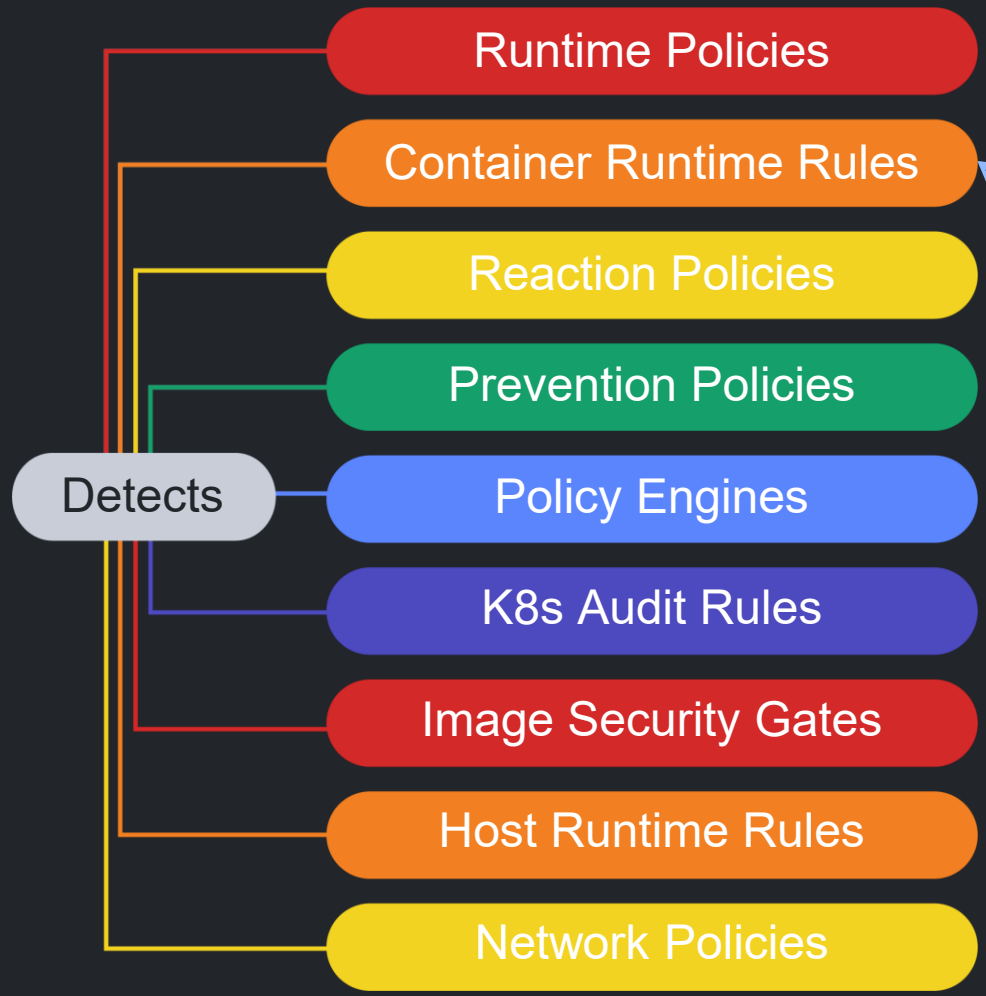
SOC FORUM 2025



Обнаружение аномалий за счет отхождения от профиля нормального поведения (whitelist)

Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025



Обнаружение подозрительной, нелегитимной, вредоносной активности (blacklist)

Сочетаем с whitelist для исключений и более строгого контроля

Пример: Обнаружение по правилу в Runtime

SOC FORUM 2025

Name: Launch Suspicious Network Tool in Container

Description:

Severity: critical

Type: Process

Date: 03.07.2025 17:16:58 (16 minutes ago)

Digest: sha256:db6adb67ad904edbfee8e438f1f60aea938ba116eaeddde32b9b2d9e2bd1ad60

Node: gimme-16ebd3d3-5

Namespace: lab-1

Pod: vulnerable-application

Container ID: b873f7354a3ce0a6156b86fdd8b9d044314de96297bdfb9162c0bc59854fc0d0

Container Name: vulnerable-application

Process exepaths: /usr/lib/jvm/java-21-amazon-corretto/bin/java /usr/bin/curl

Detect Info:

GID: 0

PID: 57684

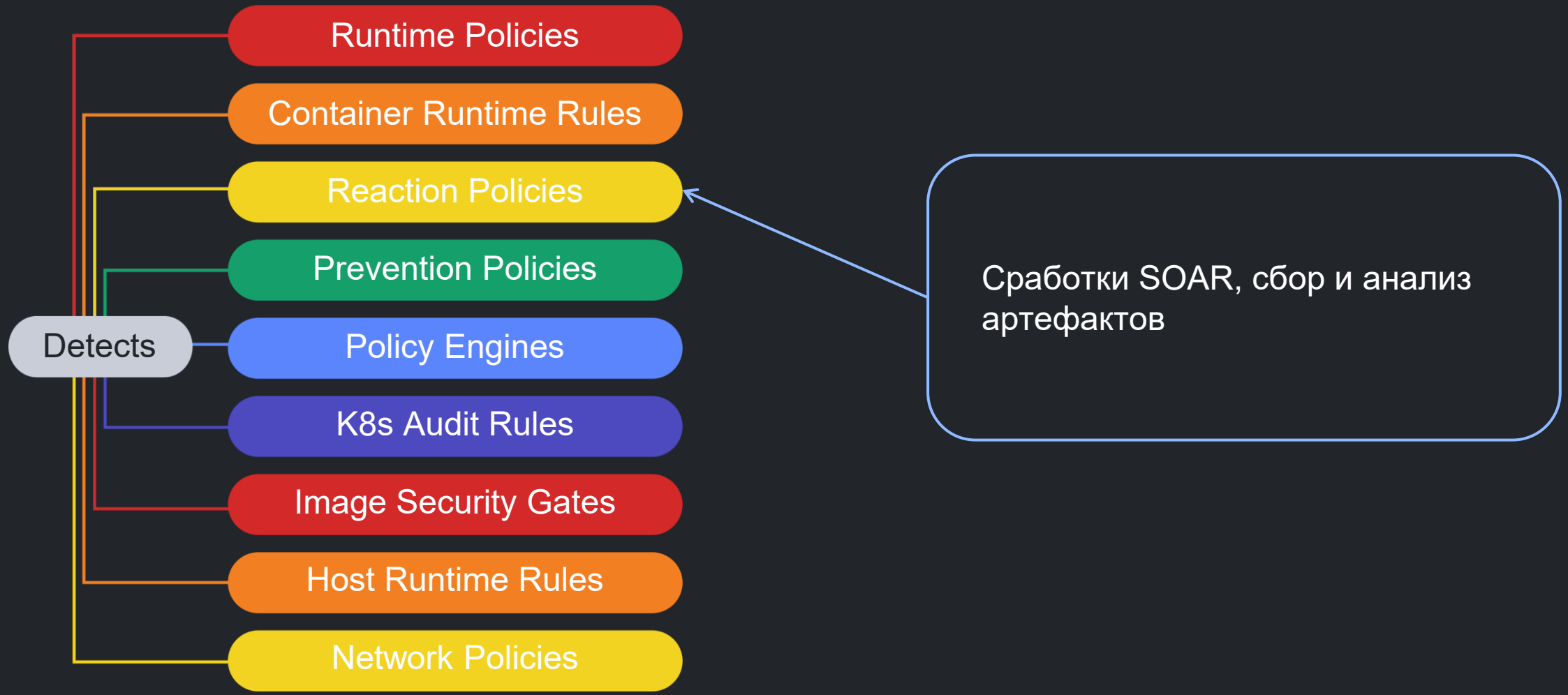
PPID: 45719

Command: curl

Arguments: --cacert /var/run/secrets/kubernetes.io/serviceaccount/ca.crt --header Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6InJ5d1JRU1hVbm9YRFU2cHZLb1JWbDRLYjB5NXJqR2FsUjg2UUd1cnFPcVEifQ.eyJhdWQiOlsiaHR0cHM6Ly9rdWJlcm

Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025

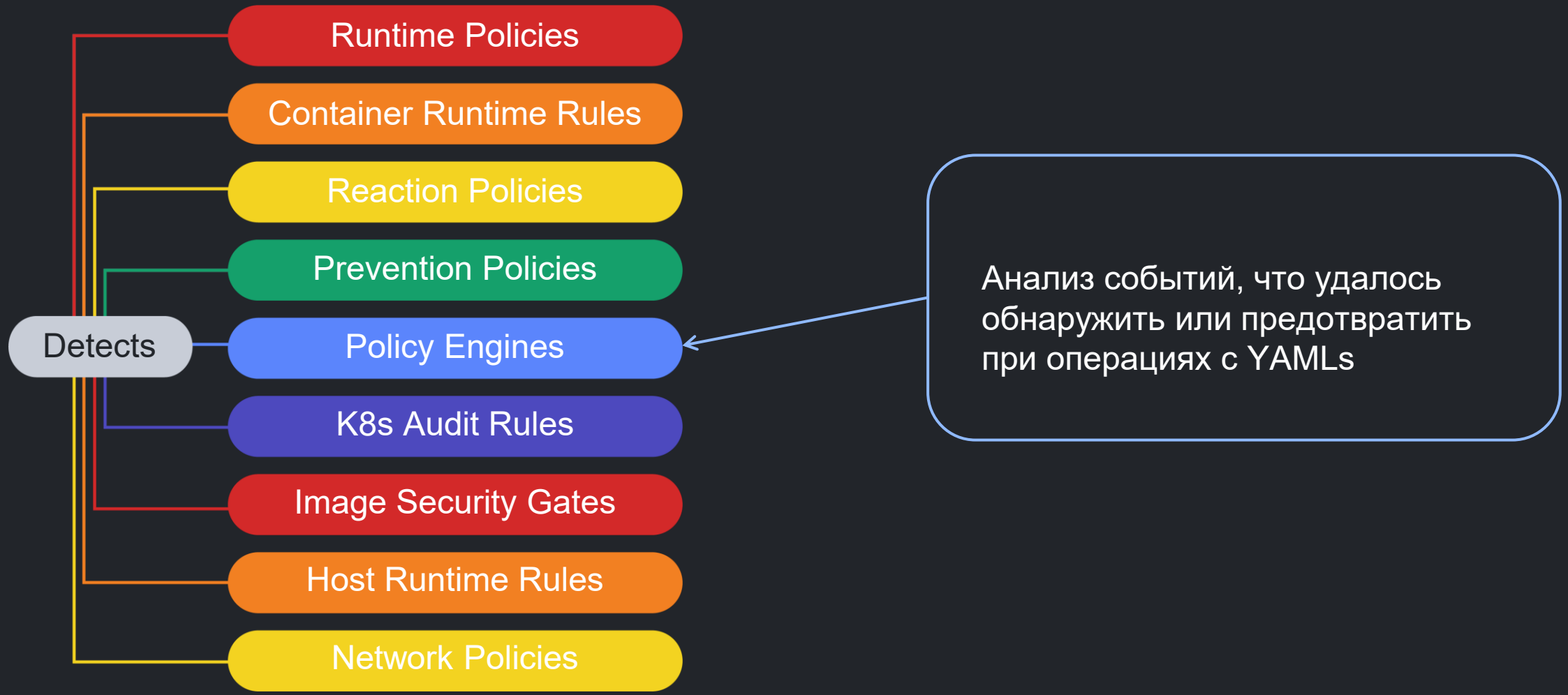


Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025

Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025

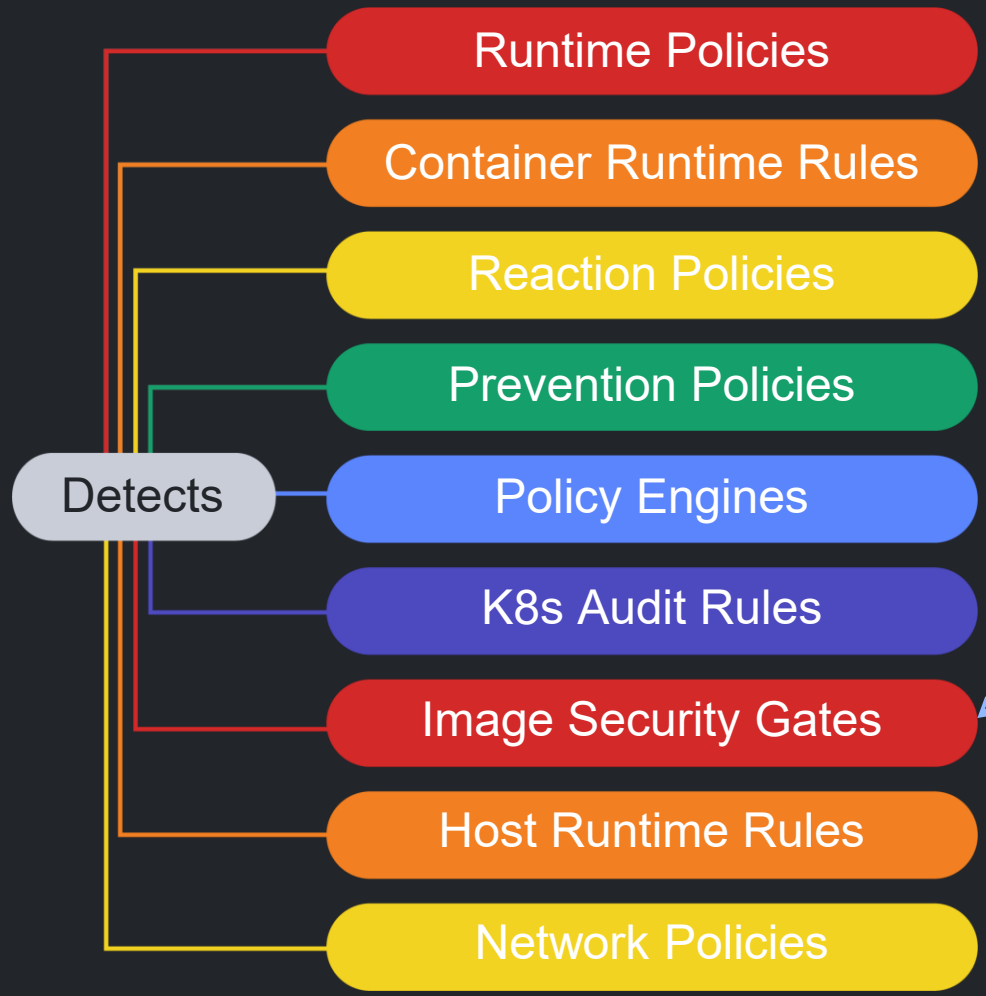


Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025

Как выглядит в целом мониторинг Kubernetes

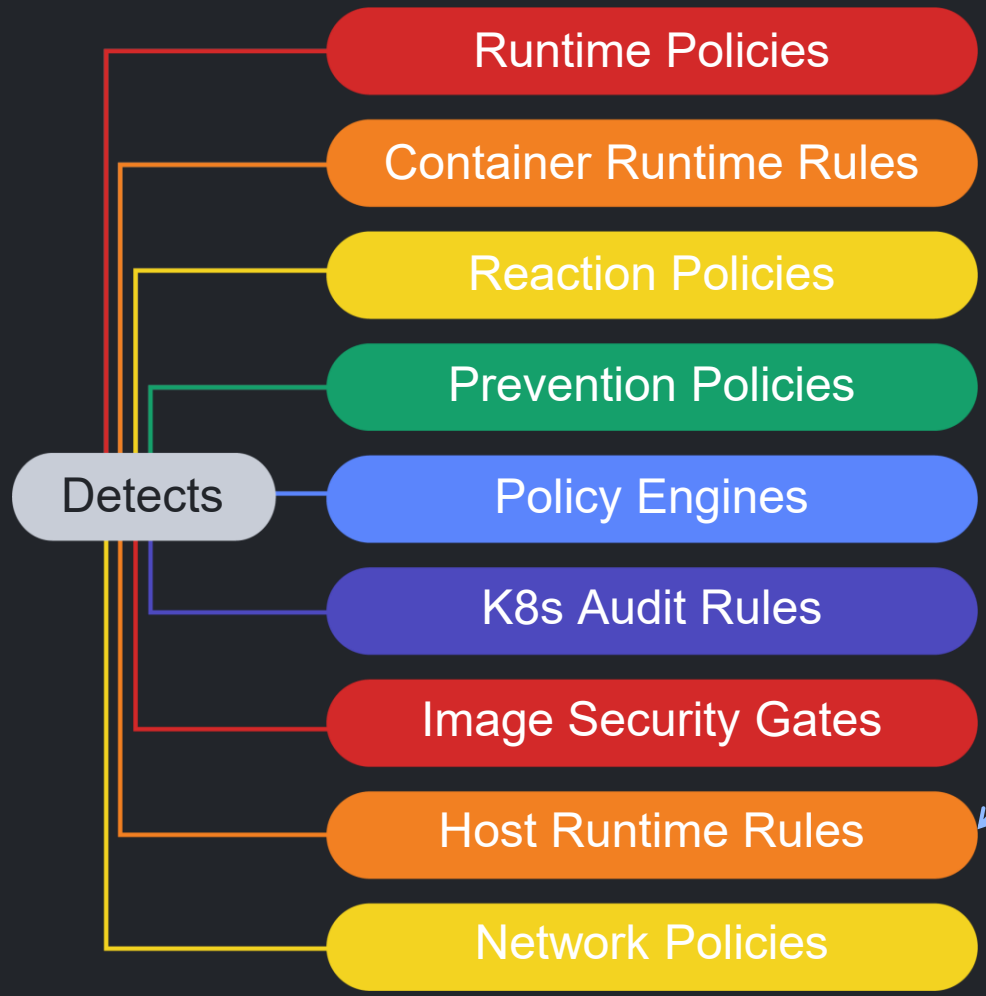
SOC FORUM 2025



Анализ событий, что удалось обнаружить относительно недостатков образов контейнеров, для обогащения других сработок

Как выглядит в целом мониторинг Kubernetes

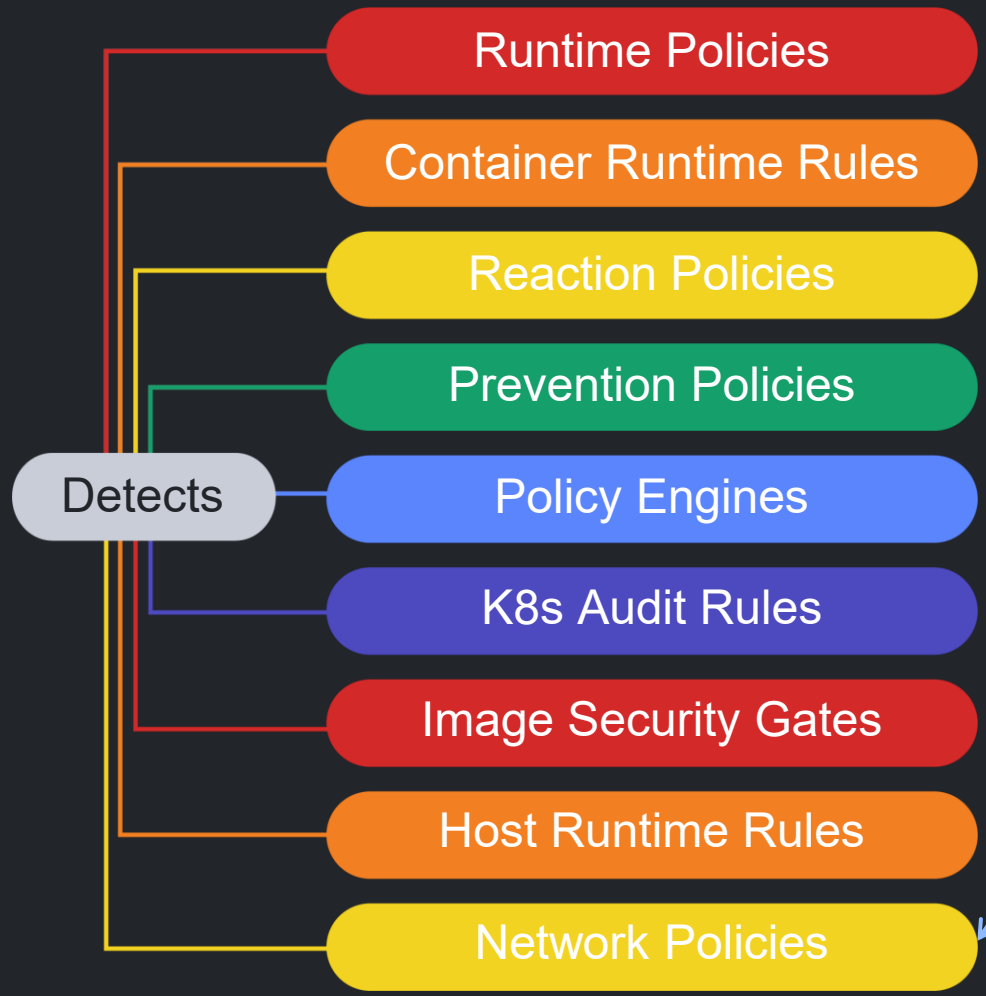
SOC FORUM 2025



Обнаружение подозрительной, нелегитимной, вредоносной активности (blacklist) на хосте

Как выглядит в целом мониторинг Kubernetes

SOC FORUM 2025



Анализ событий, что удалось предотвратить на сетевом уровне с помощью NetworkPolicy

Каким образом можно забирать события?

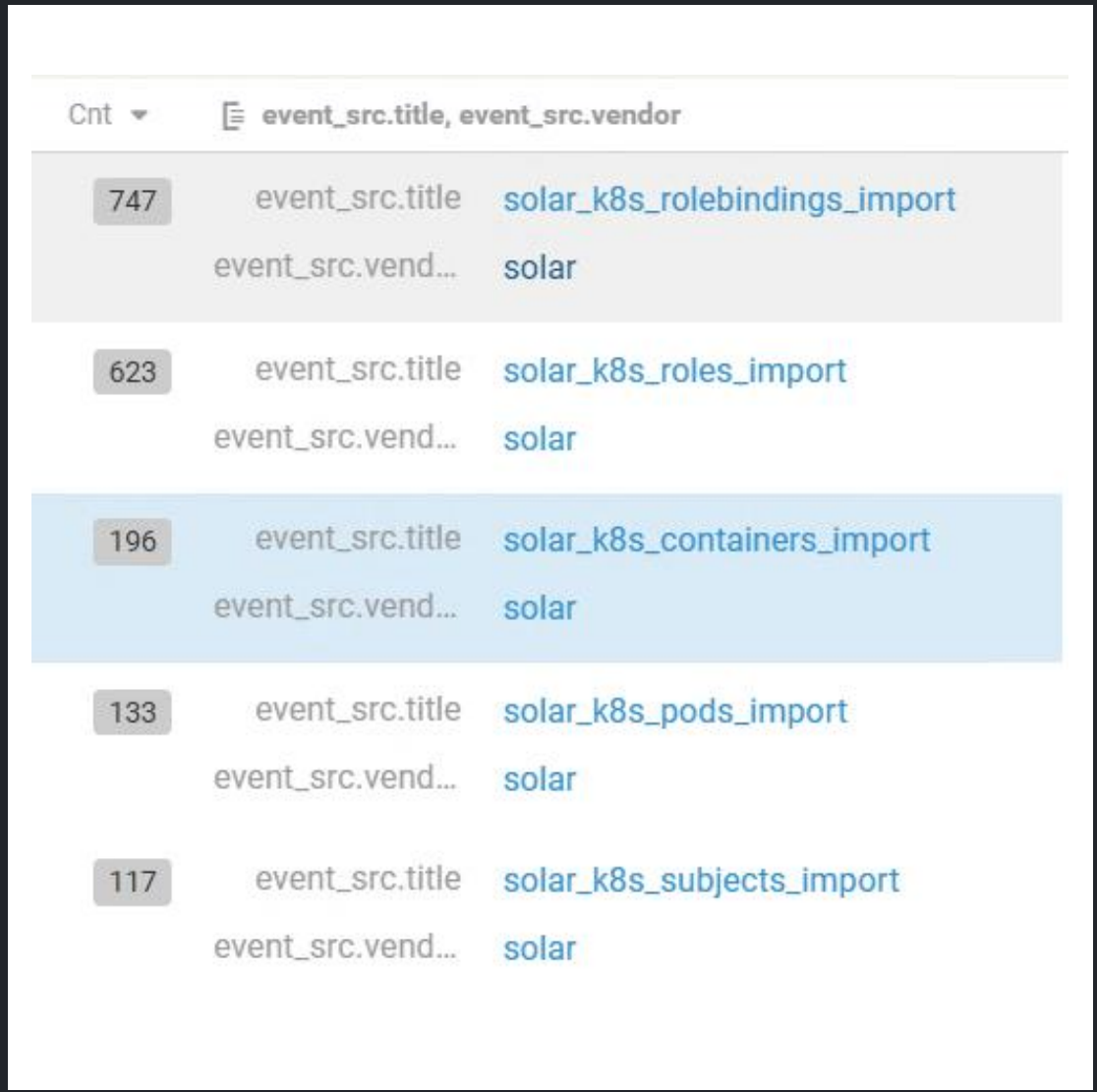
SOC FORUM 2025

API СЗИ	Как правило дает максимум информации Требуется разработка скрипта сбора в 99% случаев
БАЗЫ ДАННЫХ	Максимально «удобный» способ сбора логов – работает «из коробки»
ФАЙЛЫ\SYSLOG	Как правило сложно для парсинга Самый «простой» в плане настройки, если он есть.

Пример: забираем данные по Inventory

SOC FORUM 2025

- Выгрузка из Kubernetes API Server
- Скрипты для выгрузки и анализа данных
- Можно отправлять в SIEM и анализировать там



Выводы по разделу

SOC FORUM 2025

01

Важно собирать не только события, но и различную инвентаризационную информацию

02

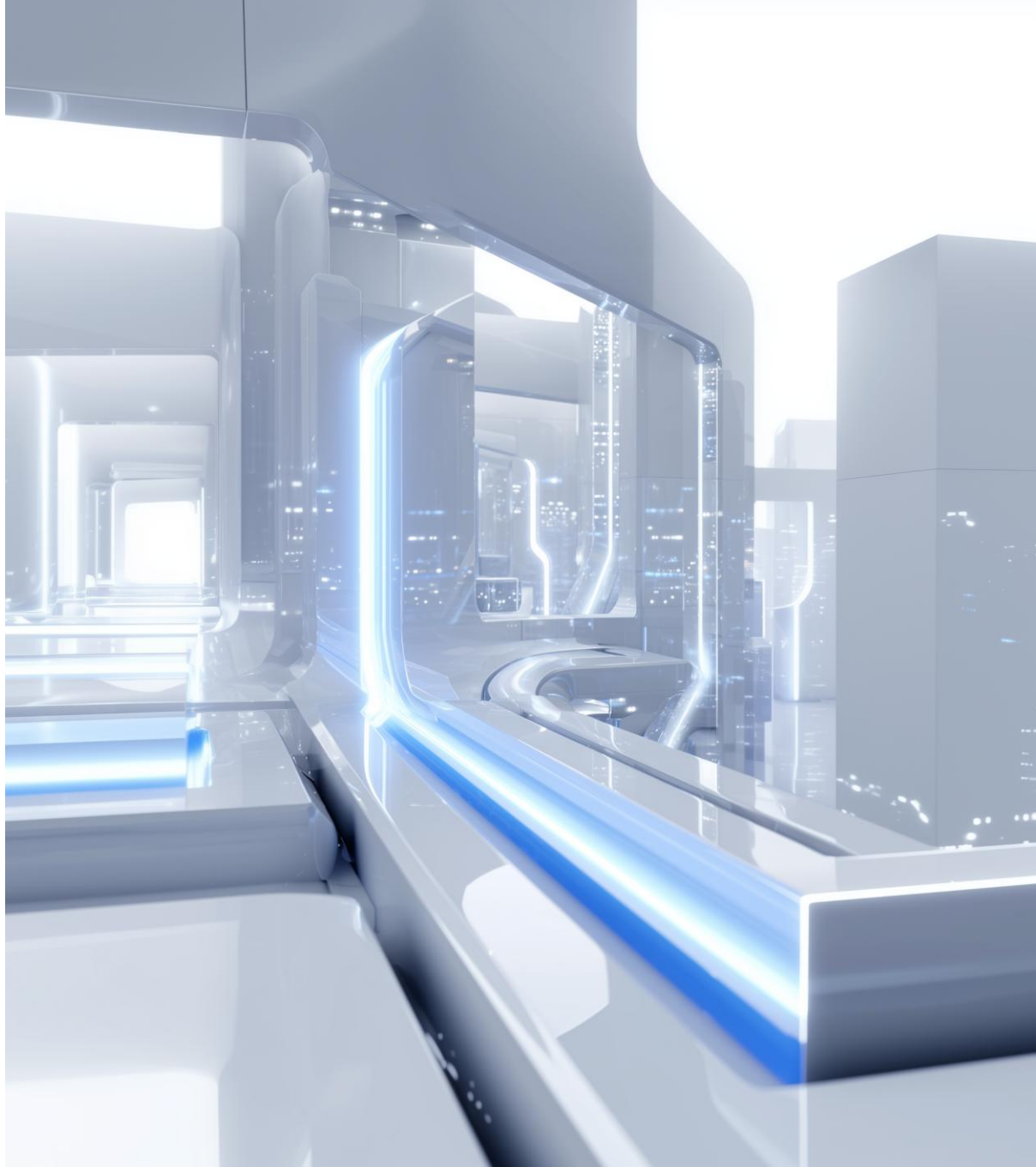
Должна быть полная связь от процесса до высокоурневого YAML ресурса

03

Важно ументь комбинировать и связывать межуд собой разные подходы

04

СТАДИЯ МОНИТОРИНГА И РАССЛЕДОВАНИЯ



Кейс 1: Знание инфраструктуры

SOC FORUM 2025

Проблема: Контейнер может при перезапуске менять адресацию. Как понять ретроспективно откуда была активность?

Решение: маппинг через инвентори \ мониторинг через СЗИ


```
{
    "allow_privilege_escalation": null,
    "capabilities": null,
    "cluster": "192.168.1.42",
    "host_port": null,
    "image": "registry.k8s.io/kube-proxy:v1.34.0",
    "is_risky": true,
    "kind": "container",
    "name": "kube-proxy",
    "node": "k8s-w2",
    "node_ip": "192.168.1.44",
    "pod_cni_ip": "192.168.1.44",
    "pod_name": "kube-proxy-9h6xc",
    "pod_namespace": "kube-system",
    "privileged": true,
    "run_as_user": null,
    "service_account": "kube-proxy",
    "volume::mount_pahts": [
        "kube-proxy::/var/lib/kube-proxy",
        "xtables-lock::/run/xtables.lock",
        "lib-modules::/lib/modules",
        "kube-api-access-jdd9x::/var/run/secrets/kubernetes.io/serviceaccount"
    ],
    "volume::mount_pahts_str": "kube-proxy::/var/lib/kube-proxy|xtables-lock::/run/xtables.lock|lib-modules::/lib/modules|kube-api-access-jdd9x::/var/run/secrets/kubernetes.io/serviceaccount"
}
```

Кейс 2: Compliance Check

SOC FORUM 2025

ЗАДАЧА

ПРОВЕРКА КОНФИГУРАЦИИ НА НАЛИЧИЕ НЕБЕЗОПАСНЫХ НАСТРОЕК.

ВАРИАНТЫ РЕШЕНИЯ:

- Можно делать через события аудита (кто-то поменял в политике X значение Y на небезопасное)
- Можно делать через выгрузку на периодической основе политик и анализ по шаблонам
- Можно смотреть по аудиту и по факту использования

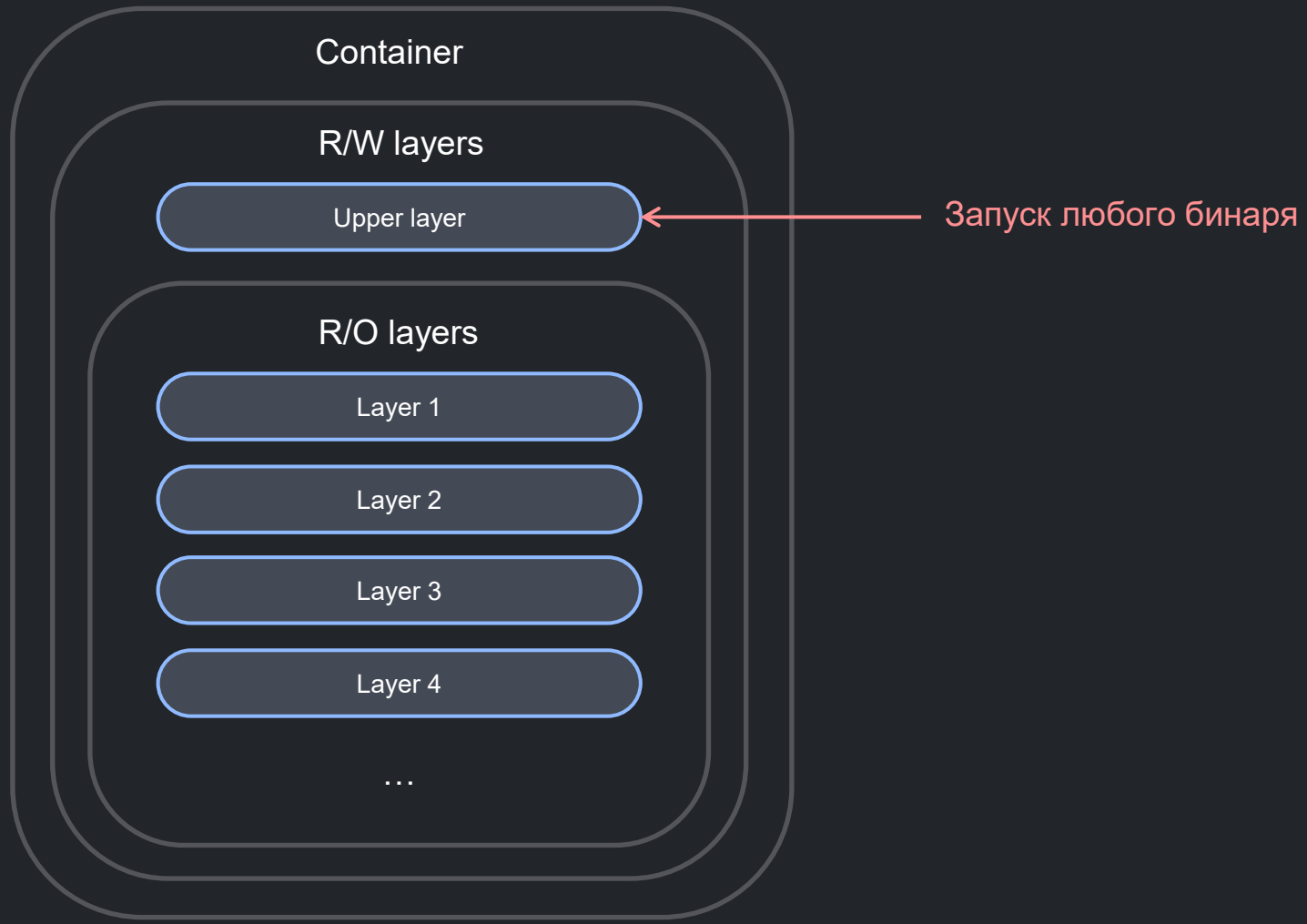
Кейс 3: Ловим новое и неизвестное

SOC FORUM 2025

Контроль запуска исполняемых файлов отсутствующих в исходном образе

- Executables drift
- Запуск с Upper layer

Не требуется никаких IOC и накладных расходов



Кейс 4: Альтернативные runtimes

SOC FORUM 2025

Runtimes с высокой изоляцией

WASM
- WasmEdge, Wasmtime, Wasmer, …

Sandbox/App kernel
- gVisor, Quark

MicroVM
- Kata containers

SOC не видит что внутри …

```yaml
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: gvisor
handler: runsc
```

```yaml
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: wasmedge
handler: wasmedge
```

```yaml
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: kuasar-vmm
handler: kuasar-vmm
```

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: gvisor-nginx
  name: gvisor-nginx
spec:
  replicas: 2
  selector:
    matchLabels:
      app: gvisor-nginx
  template:
    metadata:
      labels:
        app: gvisor-nginx
    spec:
      runtimeClassName: gvisor
      topologySpreadConstraints:
      - maxSkew: 1
        topologyKey: kubernetes.io/hostname
        whenUnsatisfiable: DoNotSchedule
        labelSelector:
          matchLabels:
            app: gvisor-nginx
      containers:
        - name: nginx
          image: nginx
          imagePullPolicy: IfNotPresent
      restartPolicy: Always
```

Выводы по разделу

SOC FORUM 2025

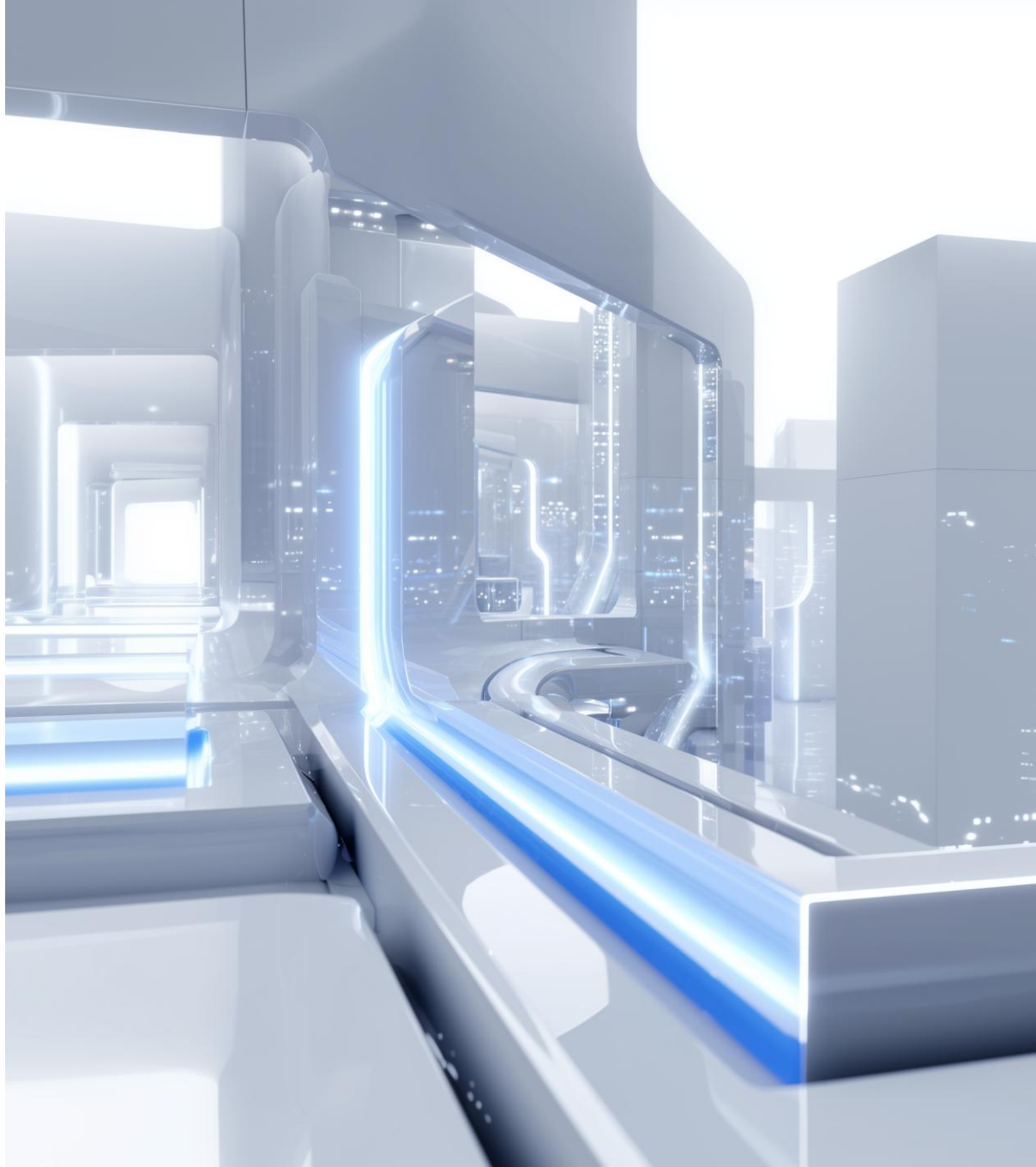
Очень важен контекст, понимание окружения, наличие истории для ретроспективного анализа

Очень большой поток данных, меняет правила игры на детектирование в runtime

Выгоднее использовать контейнерную специфику

05

СТАДИЯ РЕАГИРОВАНИЯ



Как начать реагировать в системах?

SOC FORUM 2025

Анализ доступных действий

Сброс сессий \ сбор артефактов \ завершение процессов \ блокировки УЗ

Анализ специфики системы

Как правильно отреагировать, не потеряв при этом возможность расследования

Контроль выполнения

Аудит нам тут тоже полезен ☺

Анализ возможности их выполнения

Можем ли запускать удаленно \ каким способом?

Разработка скриптов \ плейбуков

Погружаем в SIEM \ SOAR

Как начать реагировать в системах?

SOC FORUM 2025

Анализ доступных действий ★

Сброс сессий \ сбор артефактов \ завершение процессов \ блокировки УЗ

Анализ специфики системы ★

Как правильно отреагировать, не потеряв при этом возможность расследования

Контроль выполнения

Аудит нам тут тоже полезен ☺

Анализ возможности их выполнения ★

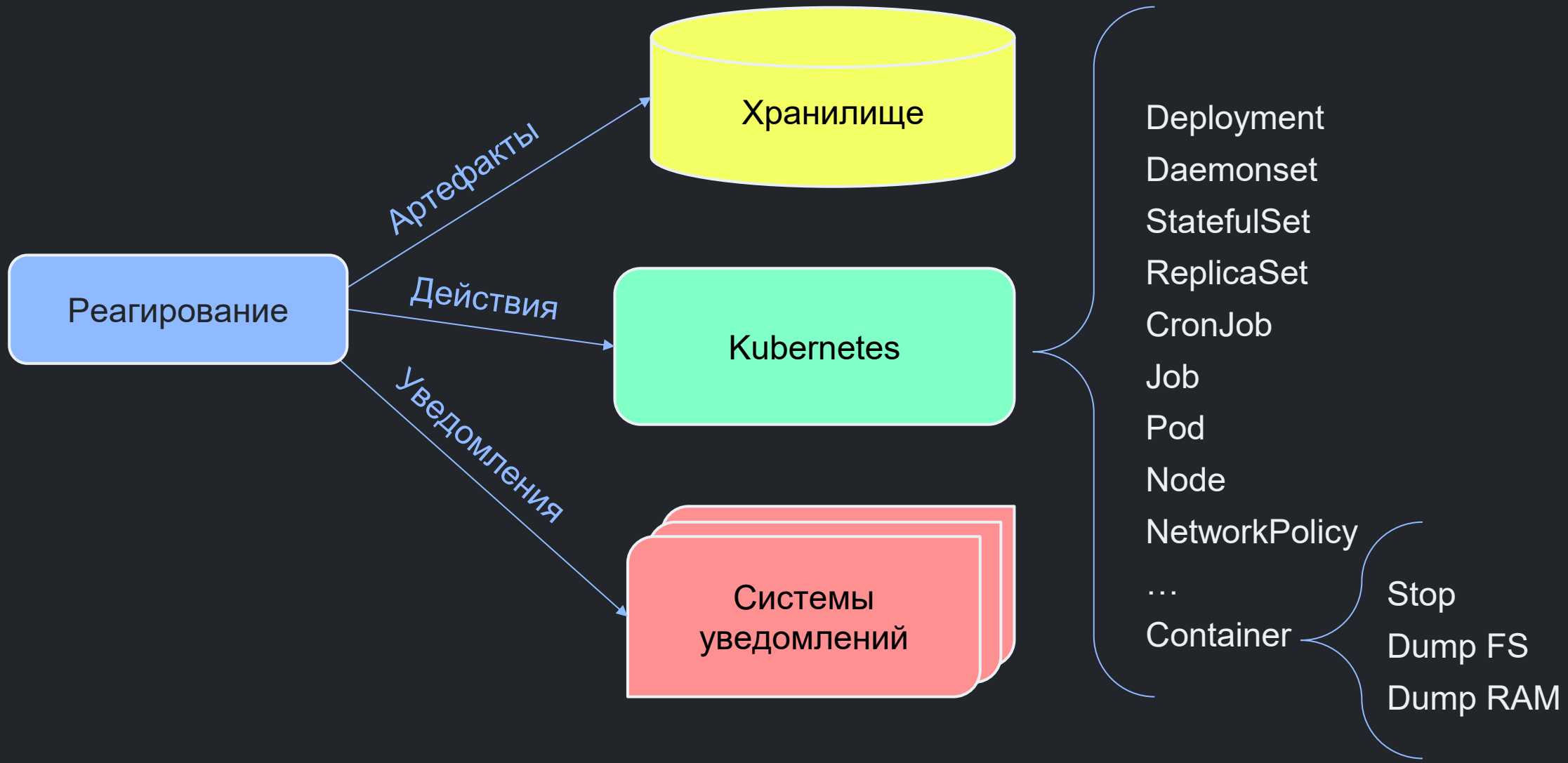
Можем ли запускать удаленно \ каким способом?

Разработка скриптов \ плейбуков

Погружаем в SIEM \ SOAR

Основные элементы реагирования

SOC FORUM 2025



Без паники!

SOC FORUM 2025

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

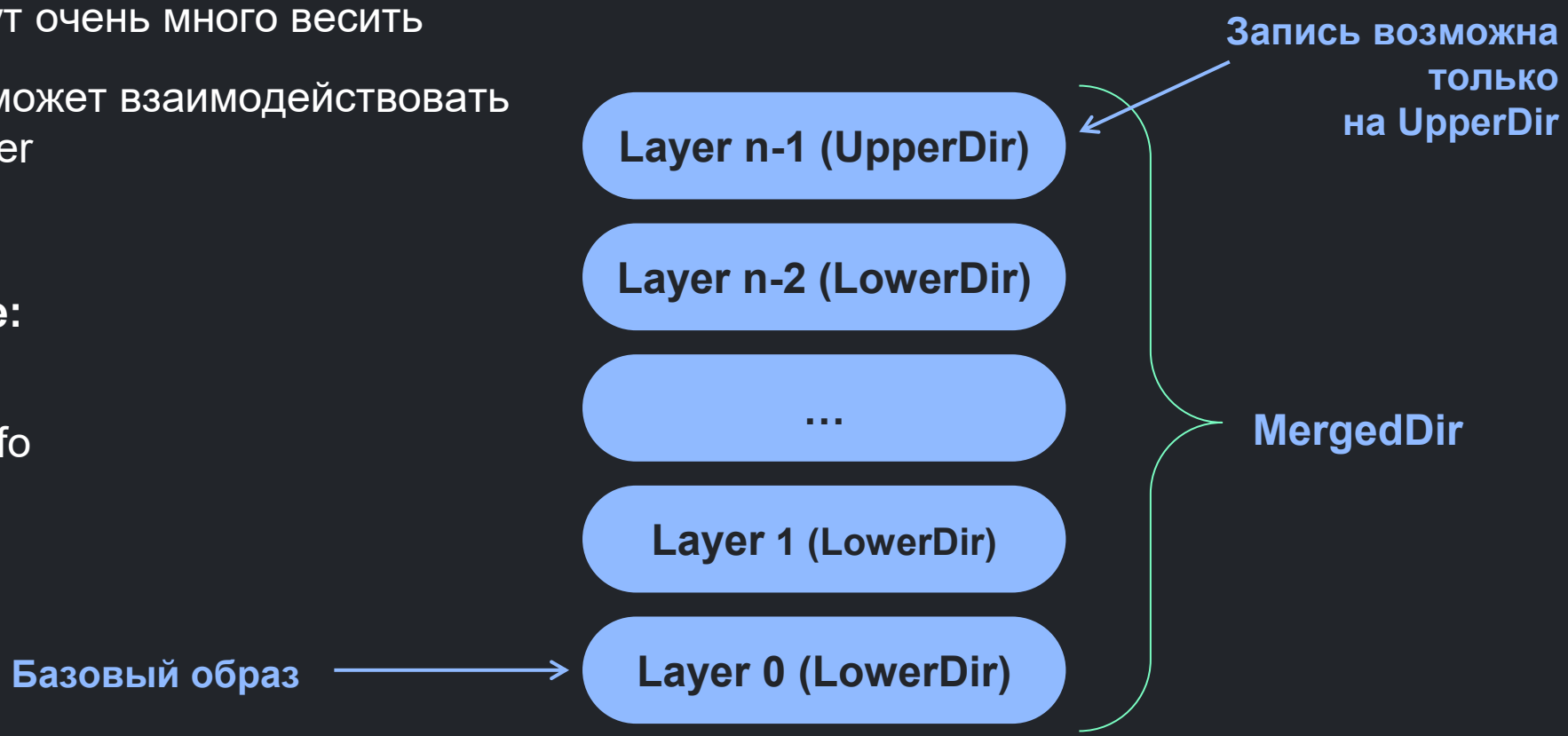
Дамп ФС контейнера

SOC FORUM 2025

1. Нет смысла дампать всю ФС целиком
2. Нижние слои могут очень много весить
3. Злоумышленник может взаимодействовать только с upper layer

Обратите внимание:

- /proc/<pid>/root
- /proc/<pid>/mountinfo
- overlayfs
- UpperDir



Выводы по разделу

SOC FORUM 2025

01

Необходимо фиксировать инциденты в контейнерах максимально быстро, пока они еще существуют

02

Сочетайте классические приемы форензики с характерными для контейнеров

03

Для эффективной форензики в контейнерных средах нужно использовать специфику контейнеров

04

Важно собирать артефакты для расследования в контейнерных окружения

SOC
FORUM
2025

ВЫВОДЫ

Выводы

SOC FORUM 2025

01

На каждой стадии есть свои подводные камни и важно знать о них и учитывать

02

SOC должен понимать контейнеры, Kubernetes как и другие системы за которые отвечают

03

Используя уникальные, сильные стороны контейнеризации и Kubernetes при построении безопасности, можно сильно снизить нагрузку на SOC

SOC FORUM 2025

rt-solar.ru

solar_security

solar_security

info@rt-solar.ru

Luntry.ru

luntry_official

luntrysolution

luntrysolution

info@luntry.ru

Максим Жевнерев
Руководитель группы развития JSOC

m.zhevnerev@rt-solar.ru

@mzhevnerev

Дмитрий Евдокимов,
Основатель & Технический директор

de@luntry.ru

Qu3b3c

k8security

СПАСИБО ЗА ВНИМАНИЕ!