Управление уязвимостями в микросервисах и контейнерных средах

Дмитрий Евдокимов

Founder&CTO Luntry

Обо мне

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- Специализация – безопасность контейнеров и Kubernetes
- CFP DevOpsConf, HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор Telegram-канала “k8s (in)security”
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Организатор конференции по безопасности контейнеров - БеКон
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, DevOops, KuberConf, VK Kubernetes Conference, HighLoad++, БеКон и др.

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/
- В процессе получения сертификата ФСТЭК

LUNTRY
luntry.ru

План доклада

- Kubernetes и контейнеры
- Уровень оркестратора
  - Уязвимости системных компонент
- Уровень приложений
  - Уязвимости пользовательских приложений
- Уровень ОС
  - Уязвимости хостовой ОС и/или ядра
- Заключение

Kubernetes и контейнеры

Kubernetes это оркестратор контейнеров

Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.

It groups containers that make up an application into logical units for easy management and discovery. Kubernetes builds upon 15 years of experience of running production workloads at Google, combined with best-of-breed ideas and practices from the community.

Pods

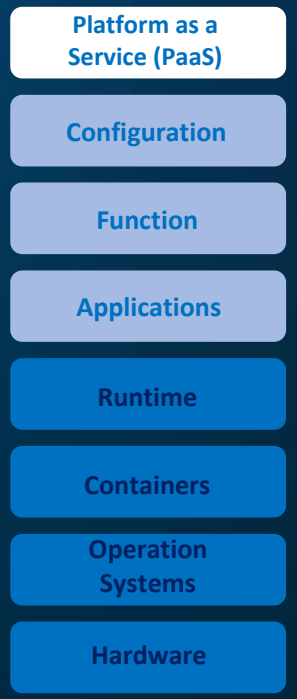
Pods are the smallest deployable units of computing that you can create and manage in Kubernetes.

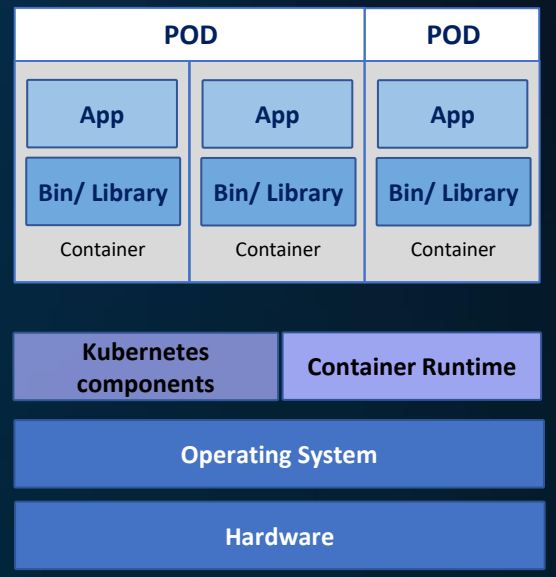
https://kubernetes.io/

Kubernetes это PaaS

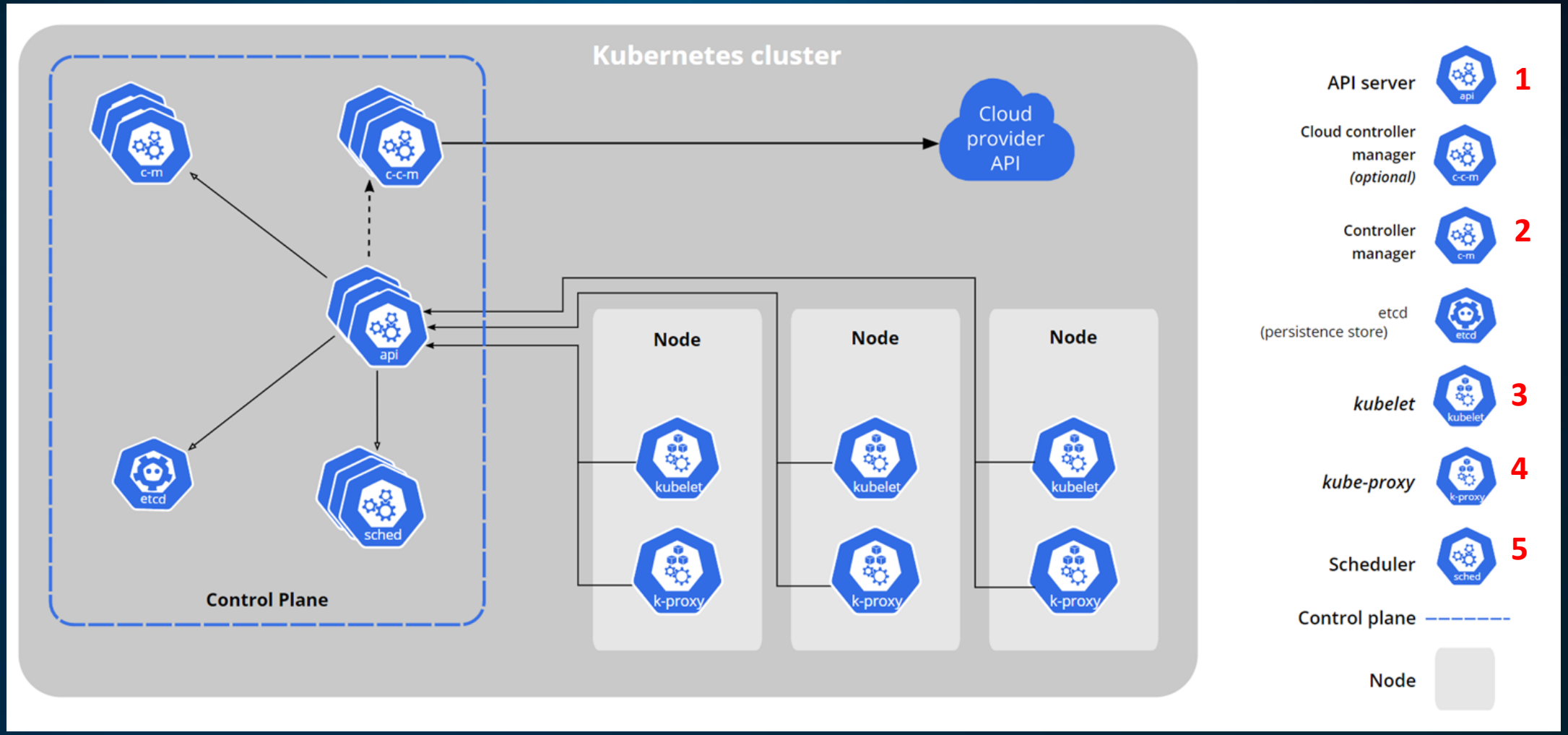
Kubernetes абстрагирован от:

- Hardware
- OS
- Containers
  - Минимальная единица управления Pod
- Runtime
  - Работает с ним через Container Runtime Interface (CRI)

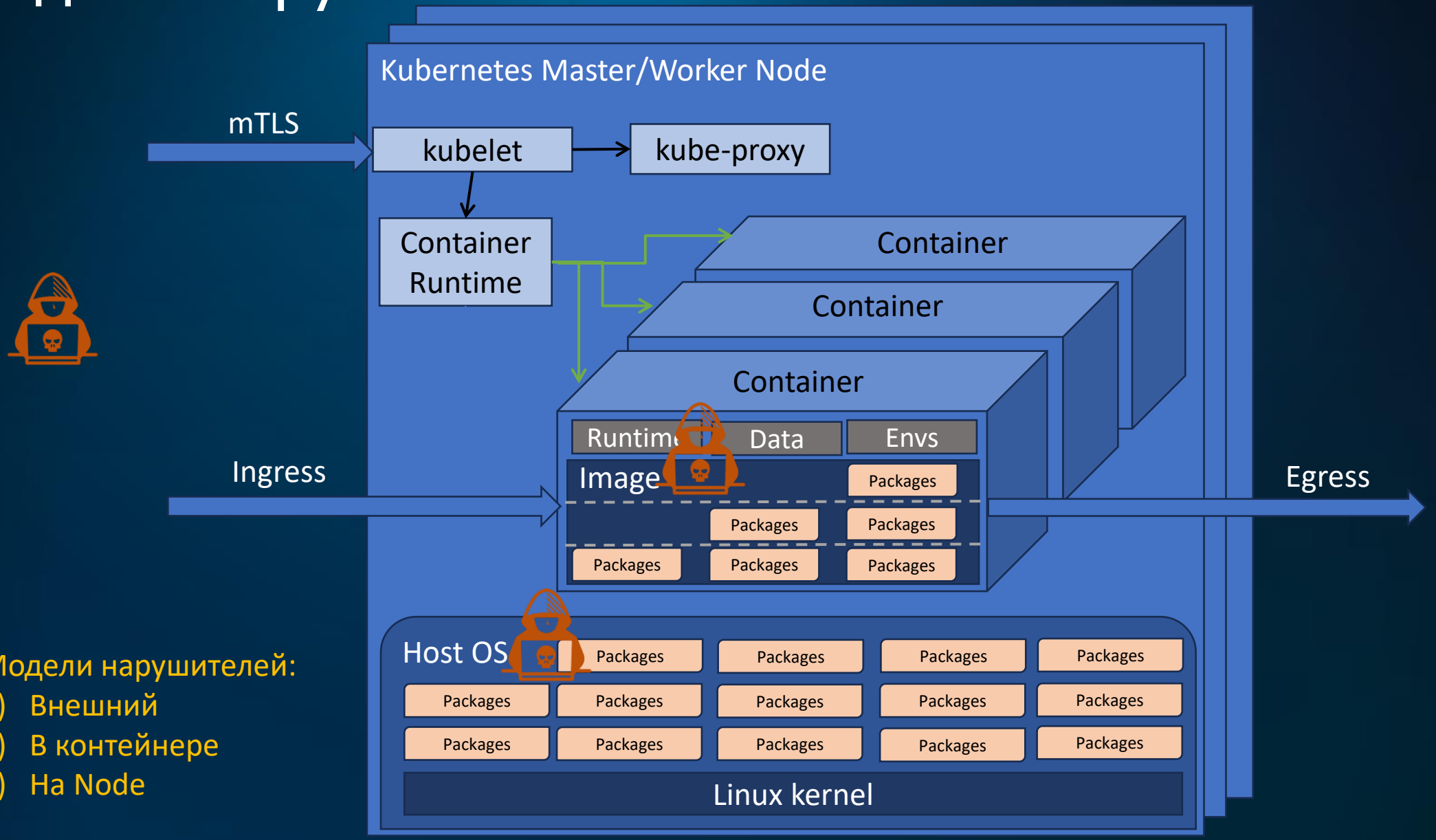




Kubernetes это 5 бинарей



Модели нарушителей

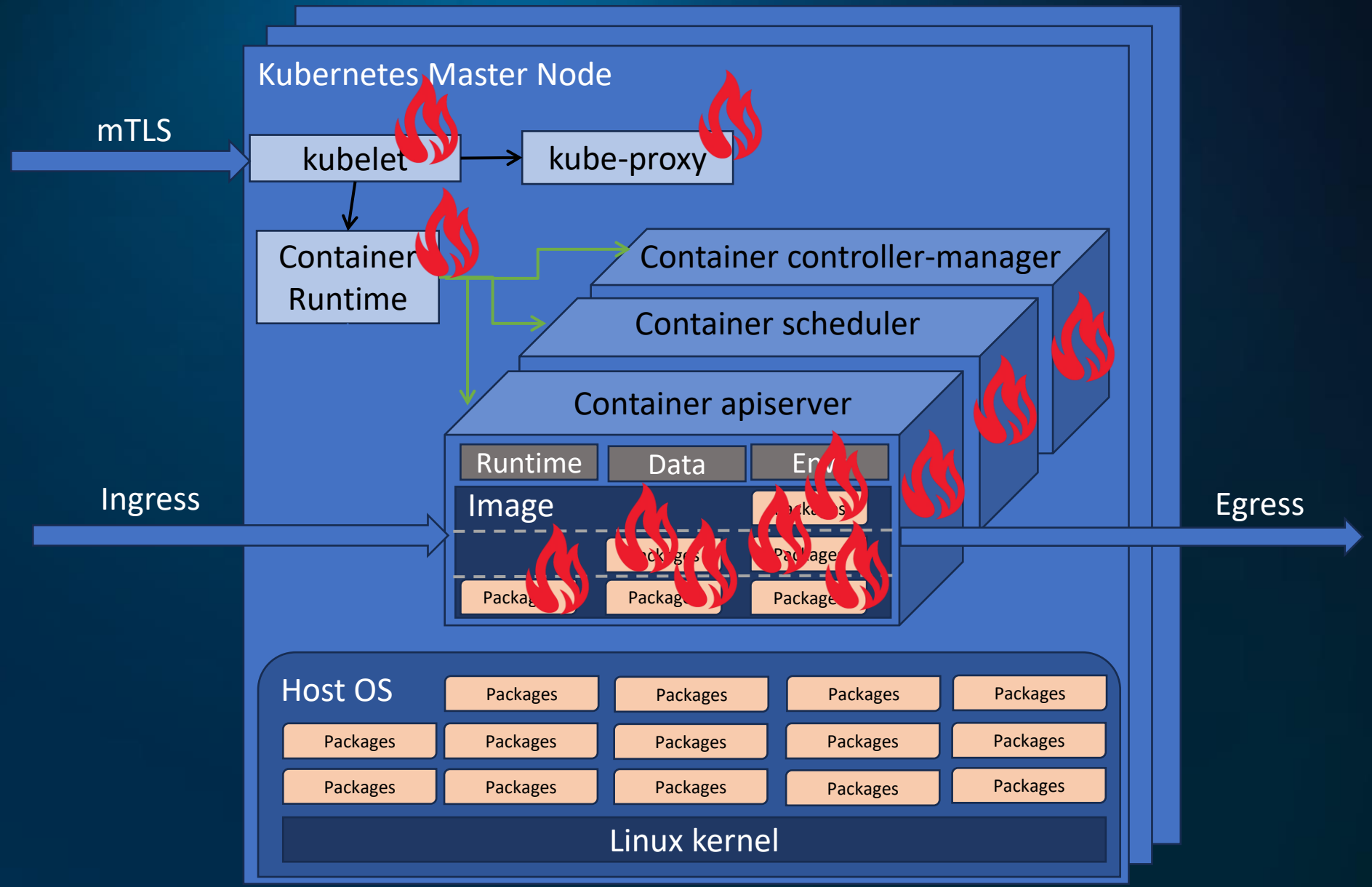


Модели нарушителей:

1) Внешний
2) В контейнере
3) На Node

Уровень оркестратора

Картина на Master Node



Официальный CVE feed и SBOM

Official CVE Feed

FEATURE STATE: `Kubernetes v1.27 [beta]`

This is a community maintained list of official CVEs announced by the Kubernetes Security Response Committee. See Kubernetes Security and Disclosure Information for more details.

The Kubernetes project publishes a programmatically accessible feed of published security issues in JSON feed and RSS feed formats. You can access it by executing the following commands:

JSON feed | RSS feed

Link to JSON format

```
curl -Lv https://k8s.io/docs/reference/issues-security/official-cve-feed/index.json
```

Official Kubernetes CVE List (last updated: 25 Mar 2024 06:38:09 UTC)

Official Kubernetes CVE List

Подпись образов и SBOM

Определение версий компонент через Kubernetes API

- API /version

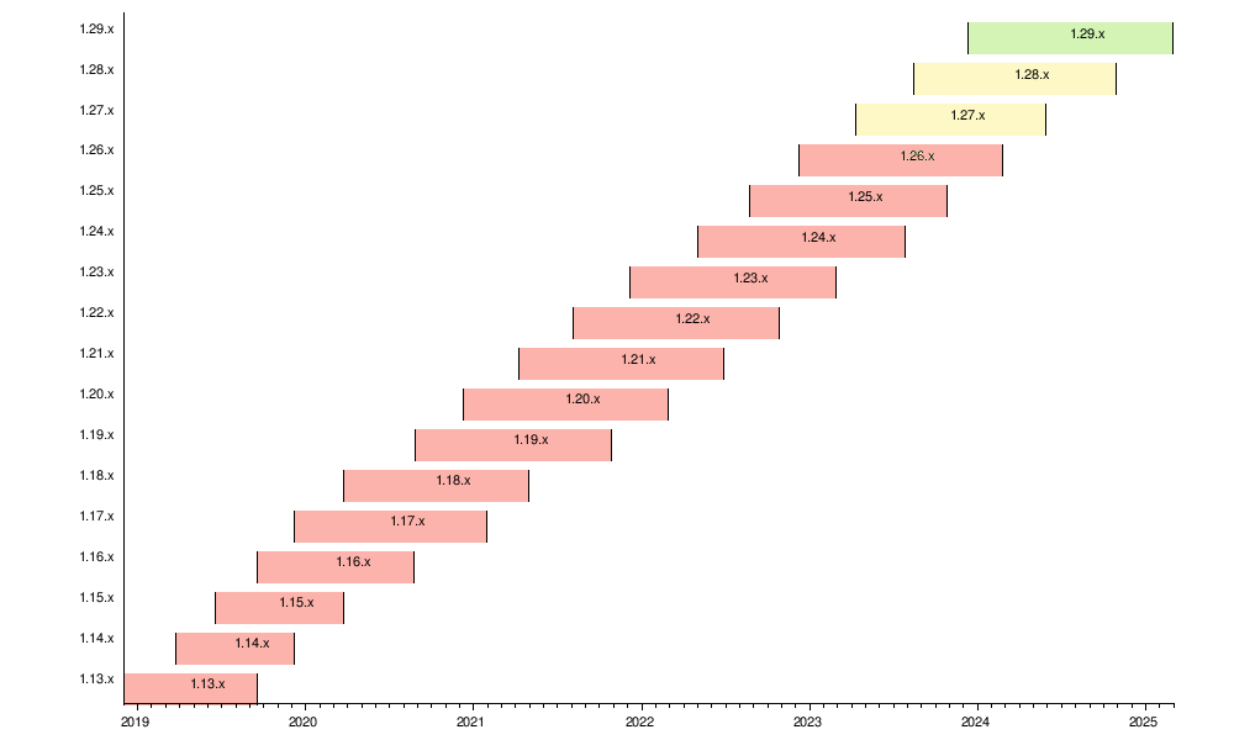
```
serverVersion:
  buildDate: "2023-08-23T23:37:25Z"
  compiler: gc
  gitCommit: 22a9682c8fe855c321be75c5faacde343f909b04
  gitTreeState: clean
  gitVersion: v1.24.17
  goVersion: go1.20.7
  major: "1"
  minor: "24"
  platform: linux/amd64
```

- Данные с ресурса Node

```
System Info:
  Machine ID:                 e6957dfff66941bfa6ad4ae19d00ea46
  System UUID:                f68a9186-d68c-4c5c-b0ce-9107193e3e8c
  Boot ID:                    f1f17565-f041-41e9-abfe-a213d9768f9d
  Kernel Version:             5.15.0-76-generic
  OS Image:                   Ubuntu 22.04.2 LTS
  Operating System:           linux
  Architecture:               amd64
  Container Runtime Version:  containerd://1.6.28
  Kubelet Version:            v1.24.17
  Kube-Proxy Version:         v1.24.17
```

Релизный цикл Kubernetes

- Поддержка последних 3-х релизов
- Поддержка релиза 14 месяцев



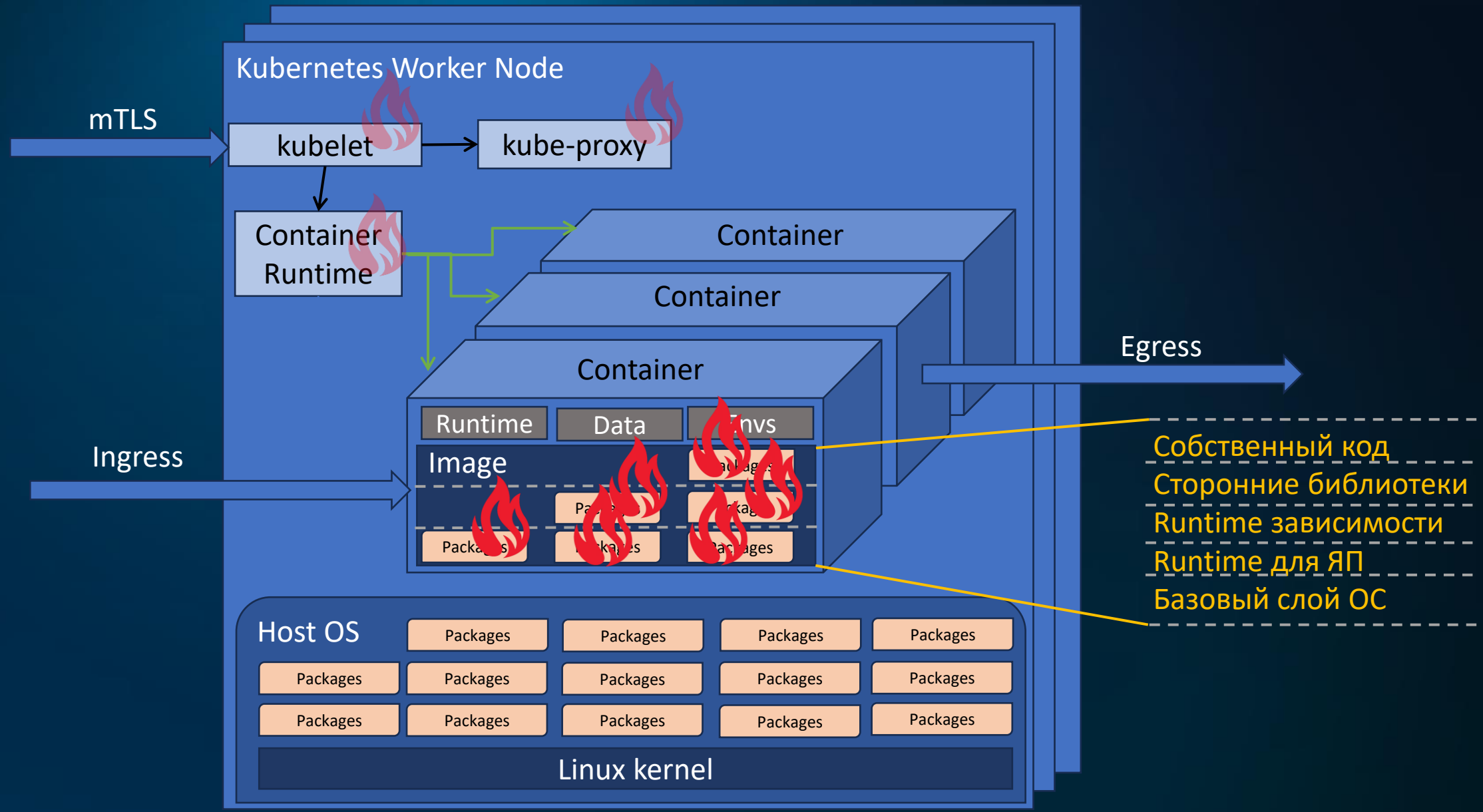
Release	Released	Active Support	Maintenance Support	Latest
1.29	3 months and 3 weeks ago (13 Dec 2023)	Ends in 8 months and 4 weeks (28 Dec 2024)	Ends in 11 months (28 Feb 2025)	1.29.3 (14 Mar 2024)
1.28	7 months ago (15 Aug 2023)	Ends in 4 months and 3 weeks (28 Aug 2024)	Ends in 6 months and 4 weeks (28 Oct 2024)	1.28.8 (15 Mar 2024)
1.27	11 months ago (11 Apr 2023)	Ends in 3 weeks and 4 days (28 Apr 2024)	Ends in 2 months and 3 weeks (28 Jun 2024)	1.27.12 (15 Mar 2024)
~~1.26~~	1 year and 3 months ago (08 Dec 2022)	Ended 3 months ago (28 Dec 2023)	Ended 1 month and 5 days ago (28 Feb 2024)	~~1.26.15 (14 Mar 2024)~~

Show more unmaintained releases

[Kubernetes Release Cycle]

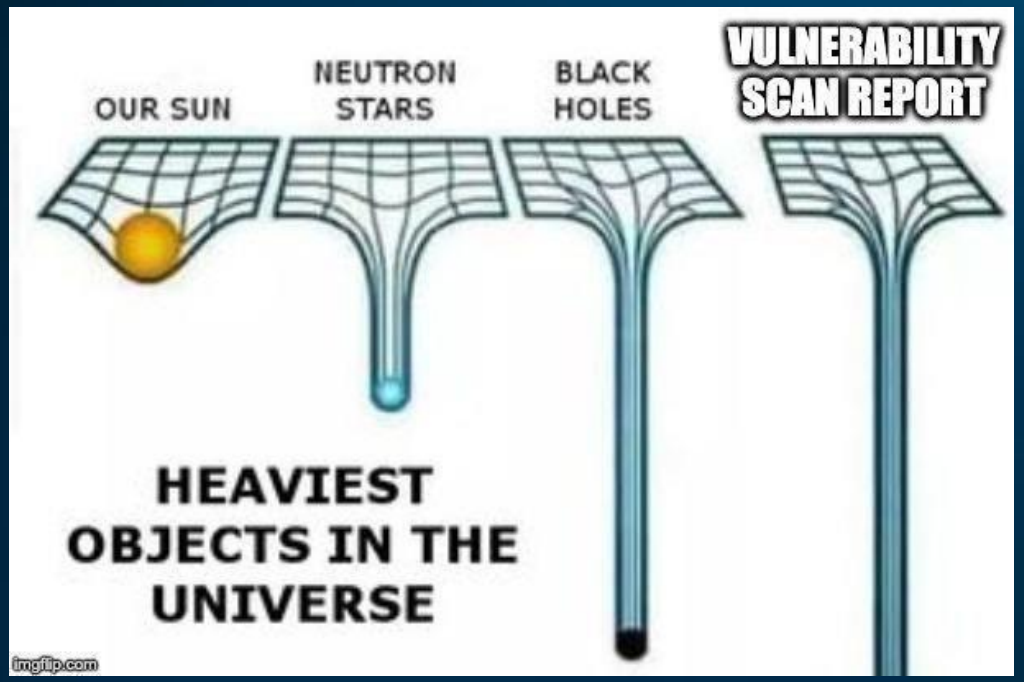
Уровень приложений

Картина на Worker Node



Анализируем образы контейнеров

- Анализ в CI\CD, image registry, runtime
- На базе SBOM
- Мало обнаружить, нужно еще исправить и выкатить в прод



Вебинар "Patch management не поможет, фиксики не спасут"

Обход сканеров

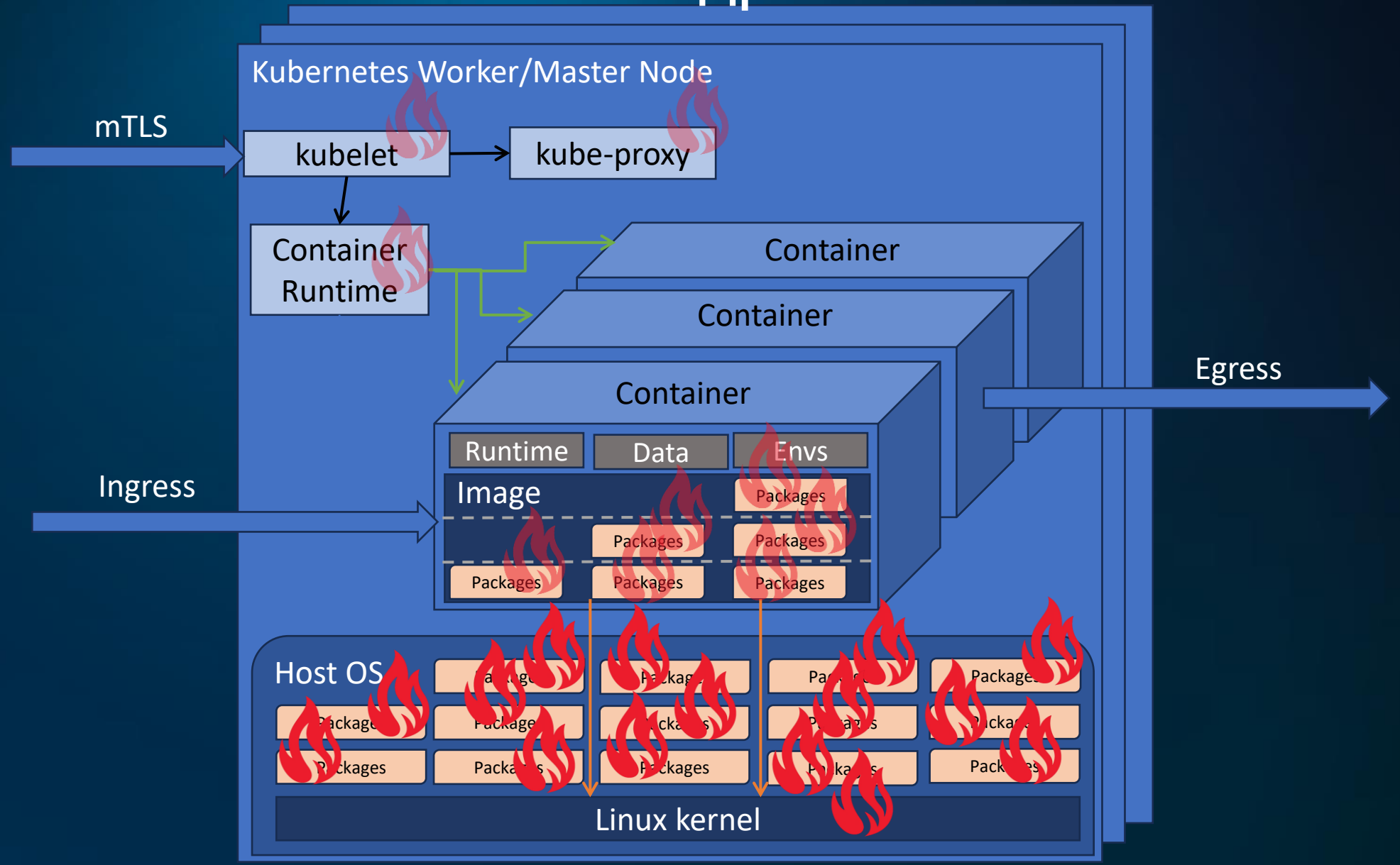
- Доклад "Malicious Compliance: Reflections on Trusting Container Image Scanners" с KubeCon EU 2023 Amsterdam.

- Все подходы на базе статического анализа позволяют защититься только лишь от легитимного пользователя, но не являются никакой помехой для вредоносного!

Серебряной пули нет

Уровень ОС

Уязвимости хостовой ОС и ядра



Уязвимости ядра хостовой ОС

- Через уязвимые системные вызовы в ядре хостовой ОС можно сбежать из контейнера на хост
  - При использовании классической контейнеризации
- Версию можно узнать через ресурс Node

```
System Info:
  Machine ID:                 e6957dfff66941bfa6ad4ae19d00ea46
  System UUID:                f68a9186-d68c-4c5c-b0ce-9107193e3e8c
  Boot ID:                    f1f17565-f041-41e9-abfe-a213d9768f9d
  Kernel Version:             5.15.0-76-generic
  OS Image:                   Ubuntu 22.04.2 LTS
  Operating System:           linux
  Architecture:               amd64
  Container Runtime Version:  containerd://1.6.28
  Kubelet Version:            v1.24.17
  Kube-Proxy Version:         v1.24.17
```

Уязвимости в пакетах хостовой ОС

- Присутствует как требование почти во всех регламентах
  - “Призвано” предотвратить компрометацию Node через известные уязвимости
- А как итог
  - Огромные отчеты об уязвимостях с большим количеством false positive-результатов
  - Огромное количество времени, потраченное дорогими инженерами на митинги и мало эффективную работу

Модель нарушителя на Node

- Root внутри контейнера равно root на Node
  - После такого побега из контейнера права повышать уже не надо
- Инженер без прав root на Node нечего делать
  - Kubernetes создан не для людей, а для контейнеров
    - Человек на Node только по экстренным ситуациям
  - Проще детектировать любую интерактивную сессию на Node, чем зависть от всех 0day и 1day уязвимостей
- Лучше вообще исключить такую модель нарушителя из своей модели угроз
  - Container specific OS приближают нас к этому еще ближе

Доклад "Безопасность Kubernetes кластеров: вредные советы"

Заключение

Итог

1. Понимайте свое окружение и модели нарушителей
2. Задача не закрыть все уязвимости, а не дать нанести ущерб
3. Специализированные системы уменьшают поверхность атаки
4. Риск-ориентированный подход наше все

Спасибо
за внимание!

Дмитрий Евдокимов
Founder&CTO


Email: de@luntry.ru


Twitter: @evdokimovds


@Qu3b3c

Channel: @k8security


Site: www.luntry.ru

k8security luntrysolution