информзащита

Информзащита
IZ:SOC

Атаки на контейнерную инфраструктуру

Тембулат Битоков
специалист отдела анализа защищенности, IZ:SOC

кибербезопасность
в эпоху перемен

Содержание

кибербезопасность
в эпоху перемен

информзащита

- Контейнерная инфраструктура
- Немного определений
- Атаки на Docker
- Атаки на Kubernetes

Who am I

кибербезопасность
в эпоху перемен

информзащита

- 2 года системного анализа
- пентестер в IZ:SOC
- багхантинг
- CTF
- s3c4rch

Дорога к мечте, ставшей явью

Bare-metal

Дорога к мечте, ставшей явью

кибербезопасность
в эпоху перемен

информзащита

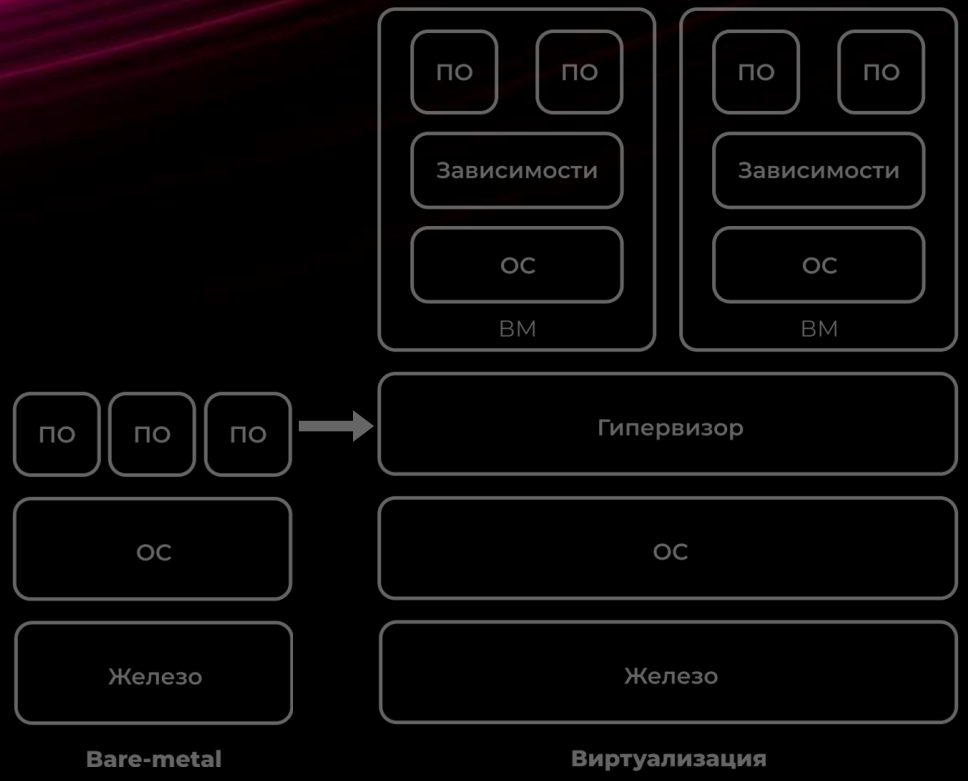
Bare-metal

Виртуализация

Дорога к мечте, ставшей явью

кибербезопасность
в эпоху перемен

информзащита

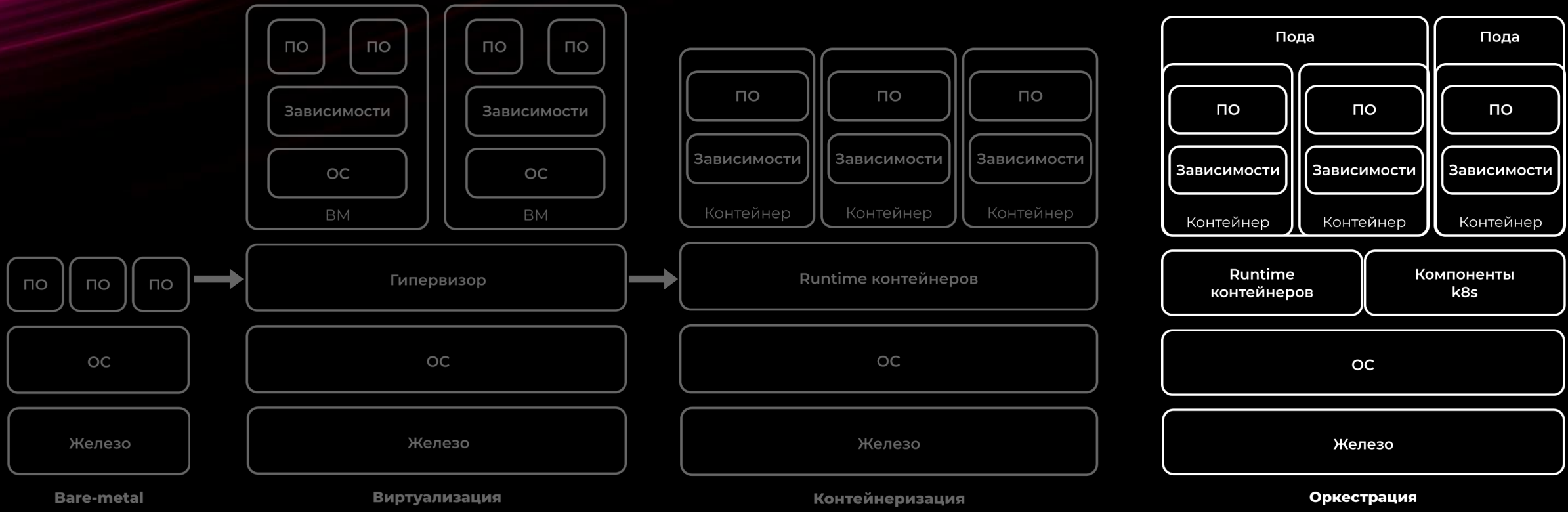


Контейнеризация

Дорога к мечте, ставшей явью

кибербезопасность
в эпоху перемен

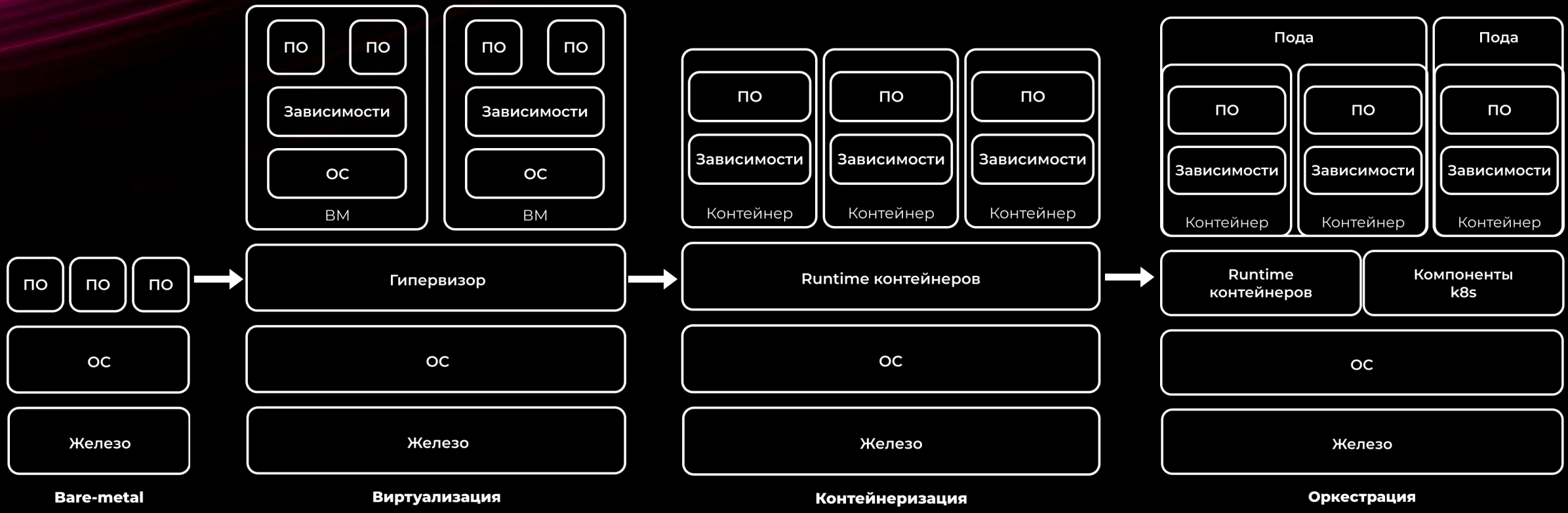
информзащита



Дорога к мечте, ставшей явью

кибербезопасность
в эпоху перемен

информзащита



for Container.Docker in Kubernetes: ?

кибербезопасность
в эпоху перемен

информзащита

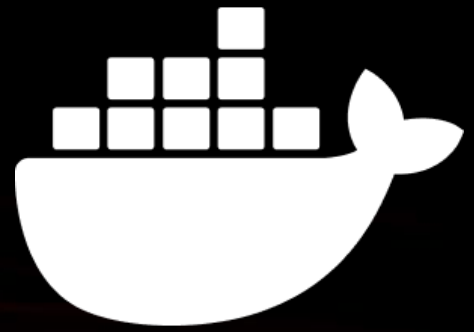
- Container = 'изолированная операционная система с необходимыми зависимостями'
- Container += 'процесс в Linux со свойствами и ограничениями'
- Kubernetes = 'ПО для автоматизации развертывания, масштабирования и управления контейнеризированными приложениями'
- Kubernetes += 'кластер — набор узлов (нод), на которых запускаются контейнеризированные приложения'

Основные векторы атак на Docker

кибербезопасность
в эпоху перемен

информзащита

- Побег из контейнера
- Использование прав суперпользователя
- Система сборки
- Общедоступные секретные данные
- Незащищённая сеть



Побег из контейнера

кибербезопасность
в эпоху перемен

информзащита

Ряд техник направленных на получение прав на хостовой машине из контейнера

например

При работе контейнеров в Linux используется cgroups — механизм ядра, позволяющий ограничивать использование, вести учет и изолировать потребление системных ресурсов (ЦП, память, дисковый ввод/вывод, сеть и т. п.) на уровне групп процессов.

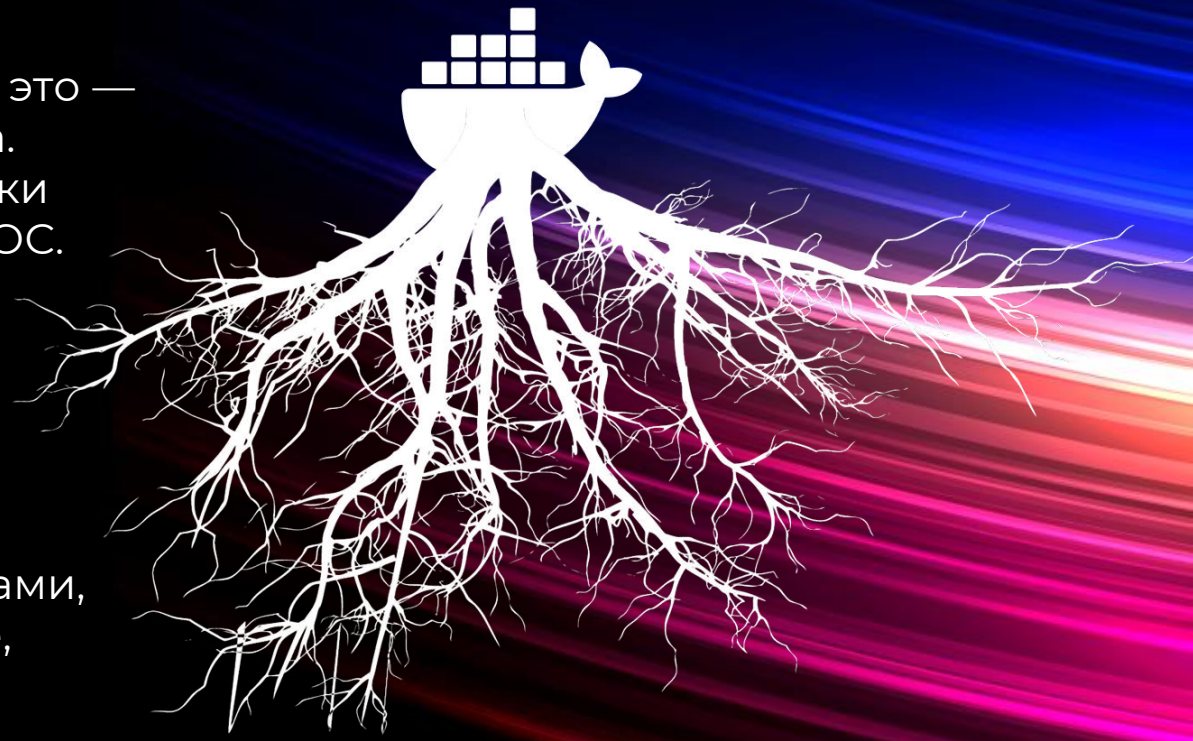
Использование прав суперпользователя

кибербезопасность
в эпоху перемен

информзащита

Самая частая небезопасная настройка контейнера это — использование root при работе внутри контейнера. Иногда такие права нужны, например, для установки и работы ПО или для внесения изменений в ядро ОС.

Опасность суперпользователя внутри контейнера заключается в следующем:
если хакер взломает приложение в контейнере,
то он сможет выполнить произвольный код с правами,
под которыми было запущено данное приложение,
то есть с правами root.



Система сборки

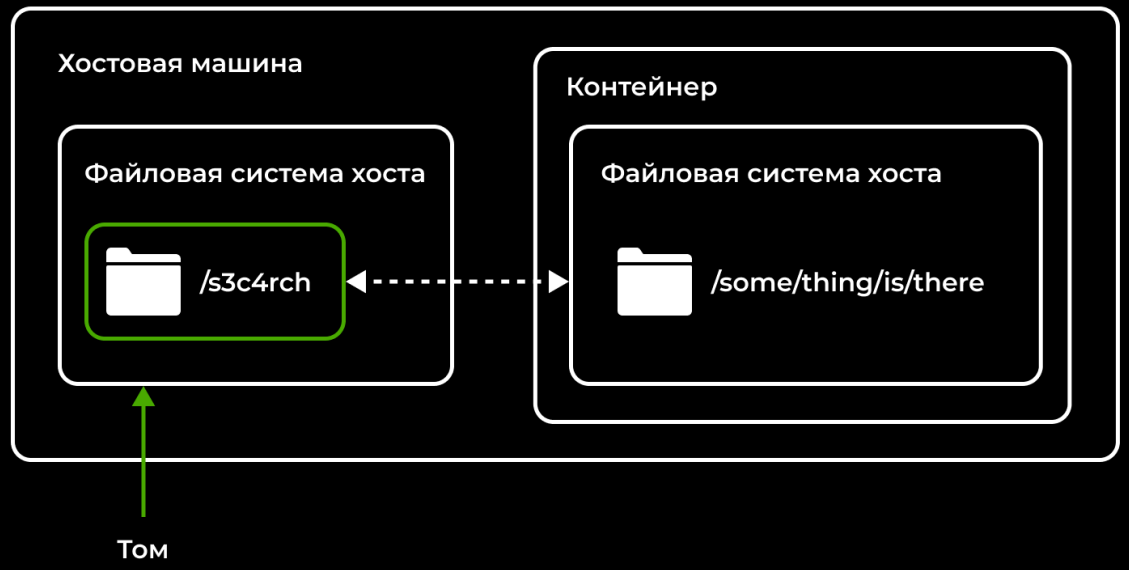
При выборе образа, на котором должен быть развернут контейнер необходимо отдавать предпочтение наиболее «лёгким» образам. Чем меньше вес образа, тем меньше вероятность наличия в нем уязвимостей.

Кроме того, небольшие образы быстрее загружаются и занимают меньше места на диске.

Ошибки при монтировании каталогов

При создании контейнеров часто используется монтирование внешних каталогов хостовой машины для хранения данных. Монтирование таких каталогов как /etc, /bin/ или /usr/bin может привести к печальным последствиям.

Так в /etc/shadow хранятся хэши паролей пользователей. Если злоумышленник проникнет в контейнер, то он получит доступ к этим подмонтированным папкам.
В /usr/bin хакер может заменить исполняемый файл, например, — ls, своим файлом.



Общедоступные секретные данные

Часто при работе различных приложений в контейнерах возникает необходимость хранения конфиденциальной информации: паролей, ключей шифрования и прочего. Разработчики используют различные способы доставки таких данных в контейнер.
Можно вшить конфиденциальные файлы в образ ОС или передавать их с помощью переменных окружения в момент запуска контейнера или в конфигурации.

Однако это не безопасные способы. Так сохранённый в контейнере файл может стать доступен злоумышленнику в случае компрометации контейнера. А при использовании переменных их содержимое может отображаться в отладочных логах. В итоге можно получить полный список всех параметров данного контейнера, включая переменные окружения.

Незащищённая сеть

кибербезопасность
в эпоху перемен

информзащита

Демон Docker для входящих API соединений использует сокет /var/run/docker.sock.
Владельцем данного ресурса может быть только root-пользователь.
Если предоставить доступ к этому сокету другому аккаунту, то данный пользователь получит root-права на этом узле.

Сокет Docker лучше не использовать. Данный сокет работает на портах 2375 (HTTP) и 2376 (HTTPS) и позволяет полностью контролировать контейнеры.
Нельзя расшаривать сокеты без крайней необходимости.

Основные векторы атак на Kubernetes

кибербезопасность **в эпоху перемен**

информзащита

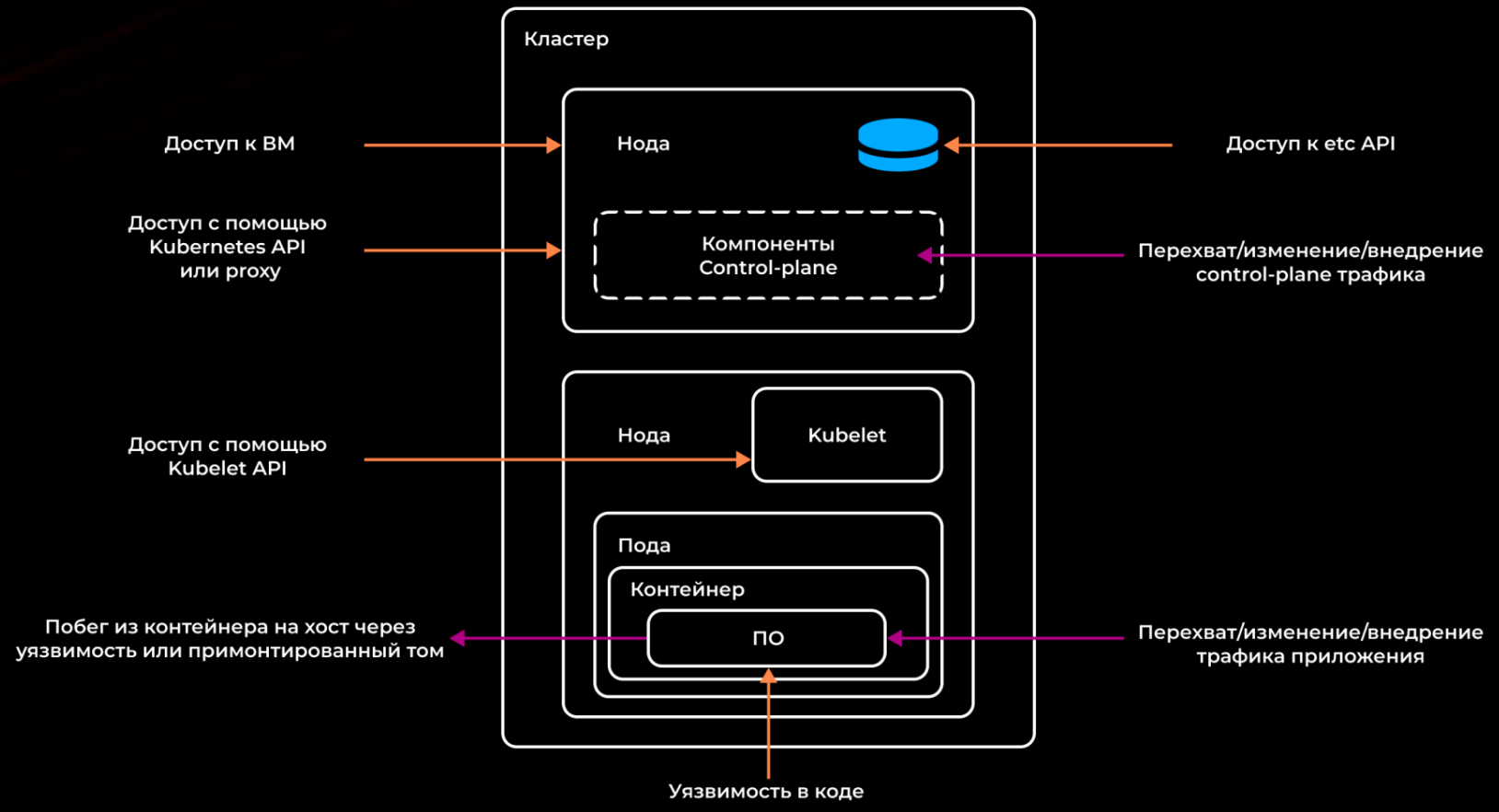
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud Credentials	Exec inside container	Backdoor Container	Privileged Container	Clear Container Logs	List K8S secrets	Access Kubernetes API Server	Access Cloud Resources	Images from a private registry	Data Destruction
Compromised image in registry	New Container	Writable hostPath mount	Cluster-admin binding	Delete Events	Access Node Information	Access Kubelet API	Container Service Account	Collecting Data From Pod	Resource Hijacking
Kubeconfig File	Application Exploit (RCE)	Kubernetes Cronjob	hostPath Mount	Pod Name Similarity	Container Service Account	Network Mapping	Cluster Internal Networking		
Application Vulnerability	Sidecar Injection	Malicious Admission Controller	Access Cloud Resources	Connect From Proxy Server	Application Credentials In Configuration Files	Exposed Sensitive Interfaces	Application Credentials In Configuration Files		Denial of Service
Exposed Sensitive Interfaces		Container Service Account			Access Managed Identity Credentials	Instance Metadata API	Writable hostpath Mount		
SSH server running inside container		Static Pods			Malicious Admission Controller		CoreDNS Poisoning		
							ARP Poisoning and IP Spoofing		

Основные векторы атак на Kubernetes

кибербезопасность
в эпоху перемен

информзащита

- Внешние атаки
- Внутренние атаки {{Пода}}
- Внутренние атаки {{Нода}}
- Атаки supply chain

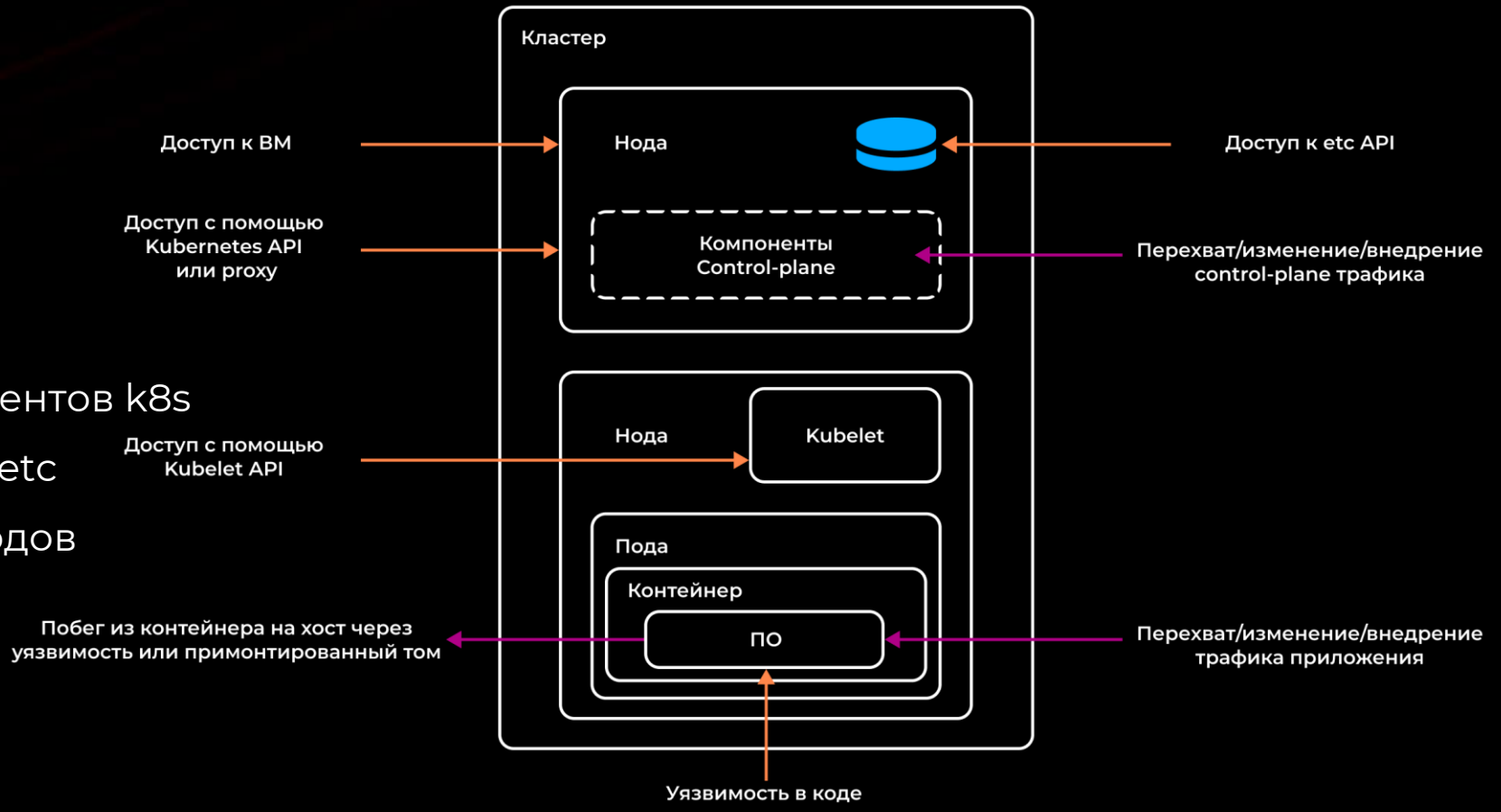


Внешние атаки

кибербезопасность
в эпоху перемен

информзащита

- Уязвимые компоненты k8s
- Уязвимые приложения
- Мисконфигурации компонентов k8s
- Мисконфигурации Docker/etc
- Мисконфигурации дэшбордов

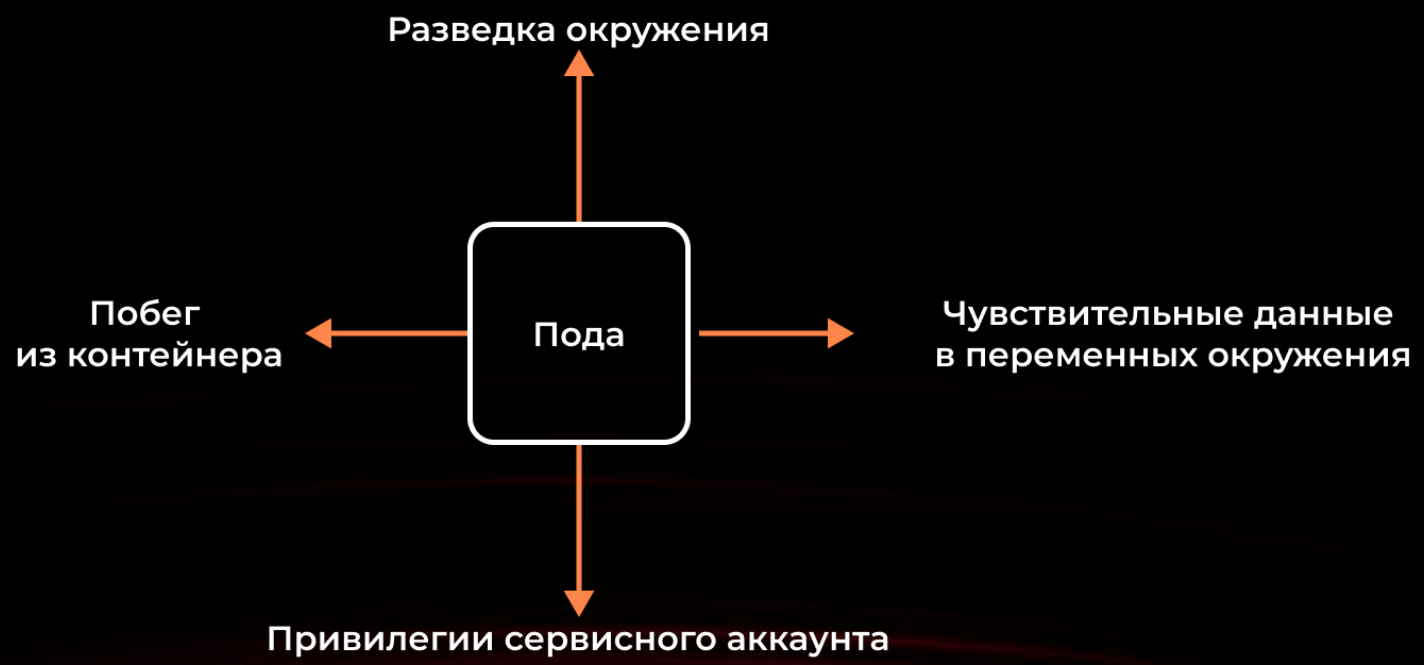


Внутренние атаки {{Пода}}

кибербезопасность
в эпоху перемен

информзащита

- Небезопасные поды
- Секреты в окружении
- Разведка у соседей (другие сервисы и компоненты)
- Привилегии

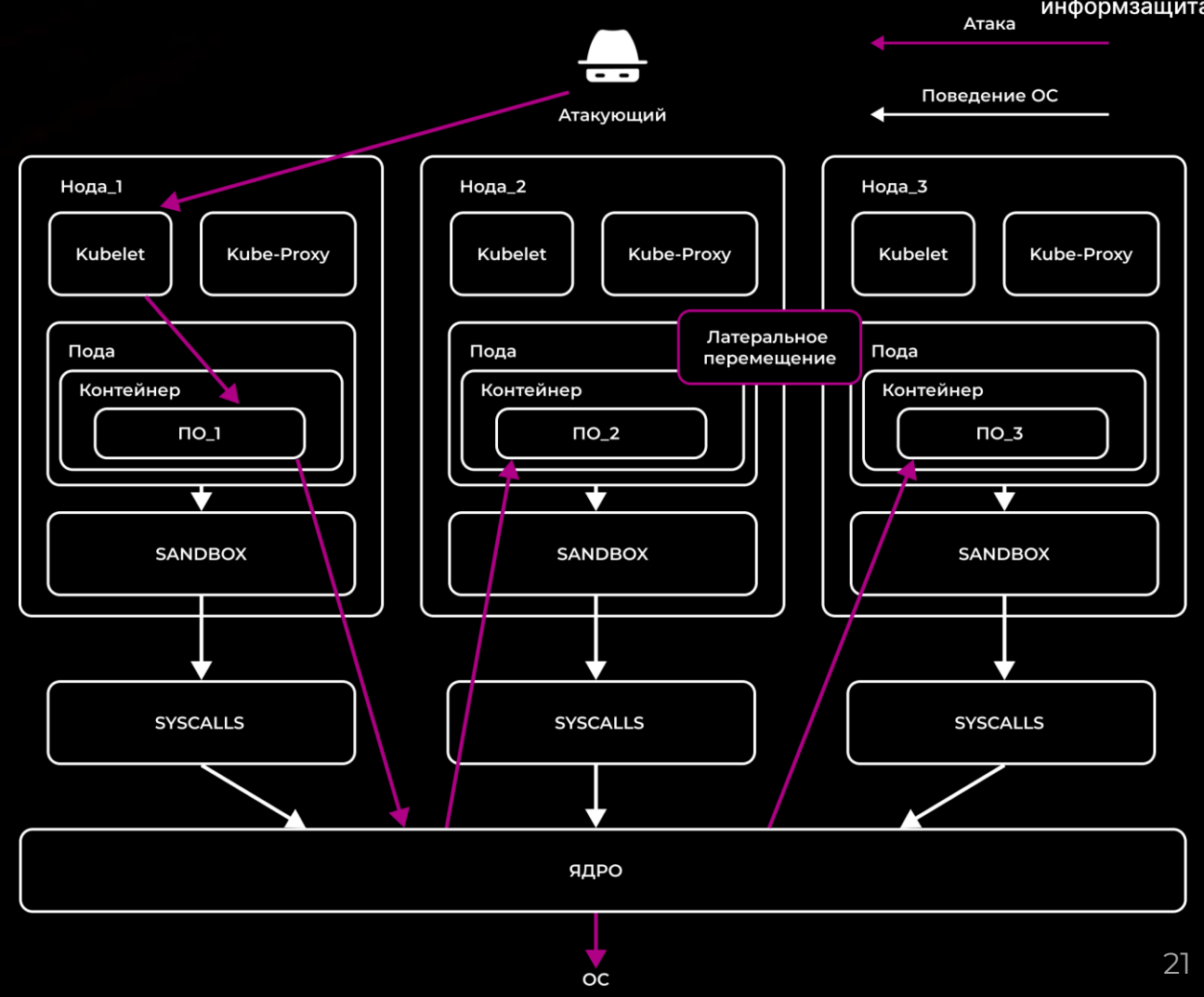


Внутренние атаки {{Нода}}

кибербезопасность
в эпоху перемен

информзащита

- Секреты (ключи/сертификаты/т.п.)
- Небезопасная сегментация

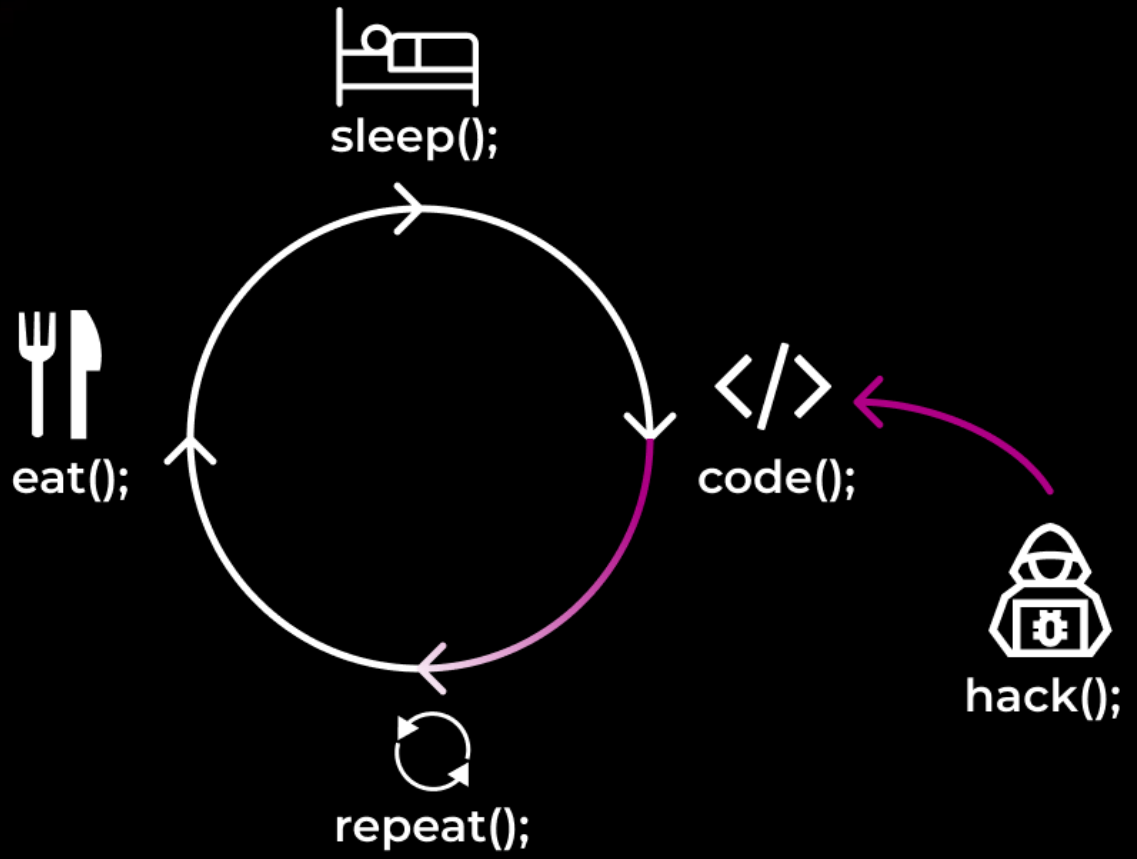


Атаки supply chain

кибербезопасность
в эпоху перемен

информзащита

- Доступ к образам (публикация в регистрах)
- Доступ к внутренним сервисам (Git, CI/CD)



Итоги *Немного статистики...

Отчет Docker, 2023

13+ млн разработчиков используют Docker
80% компаний из списка Fortune 100 внедрили Docker

Отчет CNCF, 2022

96% организаций используют Kubernetes
77% компаний применяют Kubernetes для prod'а
59% используют мультикластерные развертывания

Отчет Red Hat, 2023

67% компаний столкнулись с инцидентами безопасности в контейнерных средах
53% атак были направлены на уязвимости
в образах контейнеров
41% — на неправильные настройки Kubernetes

информзащита

Атаки на контейнерную инфраструктуру

Тембулат Битоков
специалист отдела анализа защищенности, IZ:SOC

кибербезопасность
в эпоху перемен