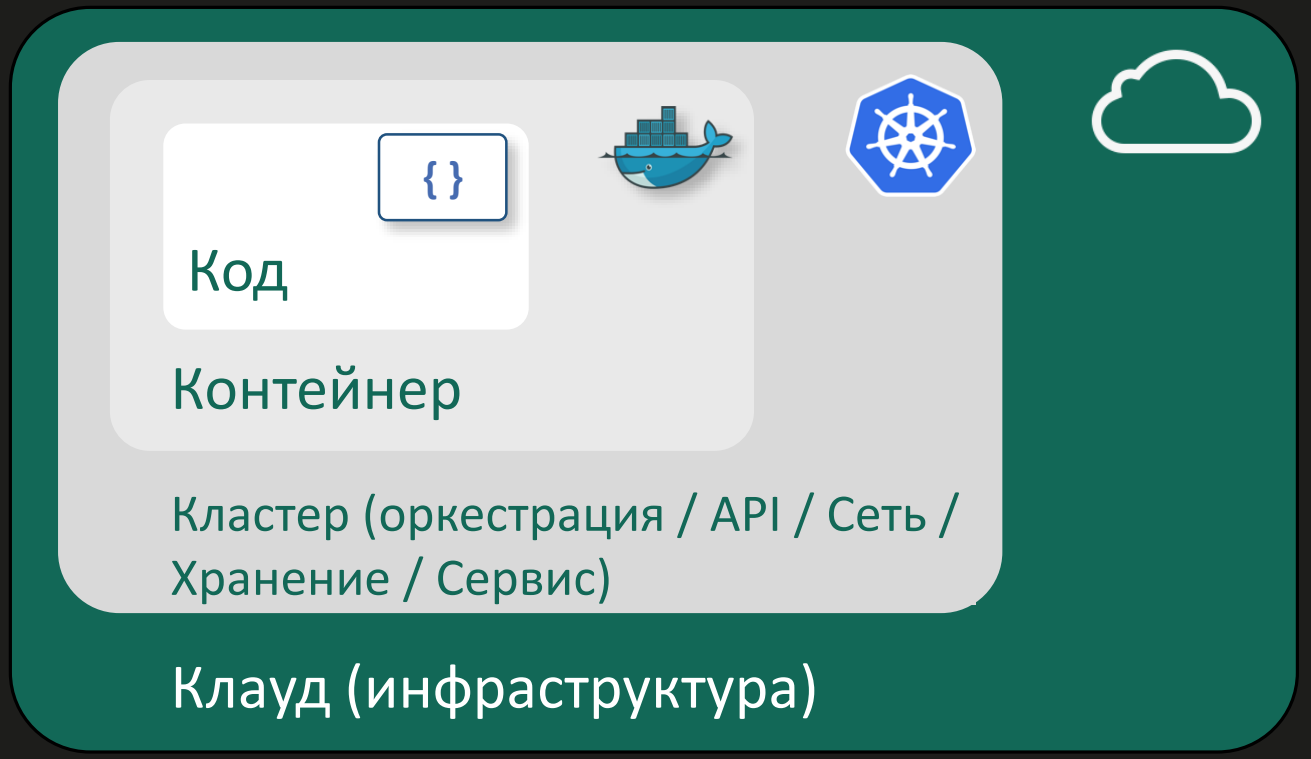
Полезные инструменты для усиления безопасности ваших контейнеров

Алексей Рыбалко
kaspersky

Почему безопасность контейнеров другая



Модель **4C** = Code, Container, Cluster, Cloud

Хранение

Сборка и запуск

Эксплуатация

Основные риски ключевых компонентов контейнерных сред

Образы

- Открытые внешние источники
- Уязвимости ПО
- Ошибки в конфигурациях
- Вредоносное ПО
- Секреты в открытом виде
- Использование не доверенных образов

Реестр образов

- Незащищенное подключение
- Наличие устаревших образов с уязвимостями и вредоносным ПО
- Недостаточные ограничения на аутентификацию и авторизацию

Оркестратор

- Административный доступ
- Доступ без авторизации
- Отсутствует разделение трафика между контейнерами
- Не разнесены по хостам контейнеры с разным уровнями защиты данных
- Ошибки в конфигурации

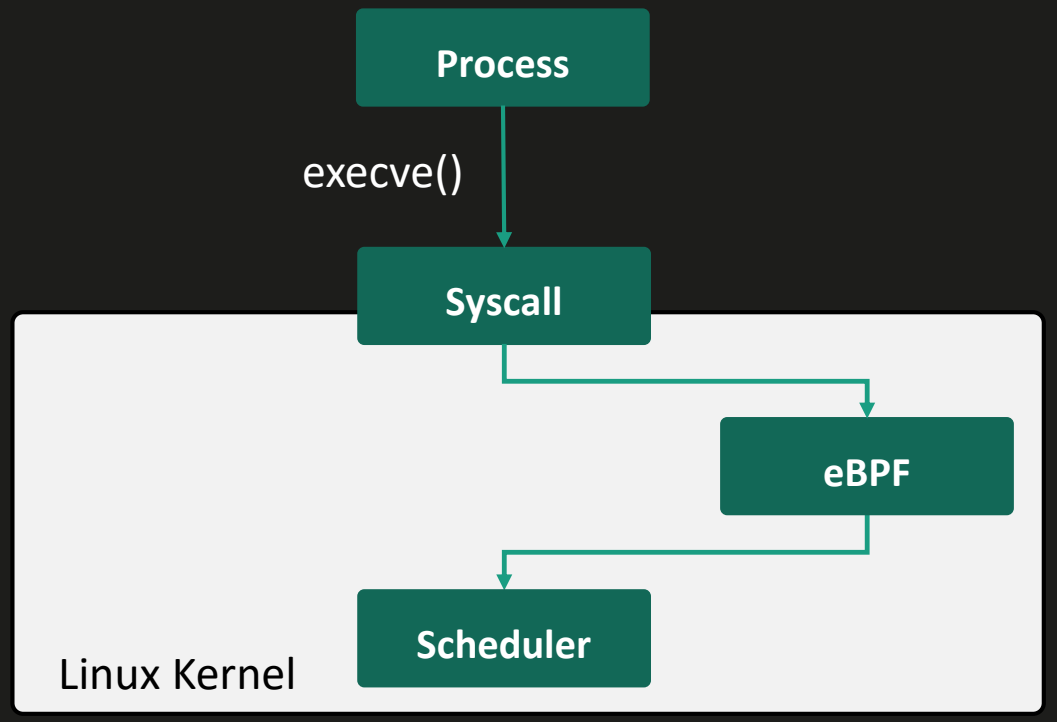
Контейнеры

- Уязвимости среды выполнения
- Неограниченный доступ контейнеров к сети
- Небезопасные конфигурации
- Уязвимости ПО в контейнерах
- Незапланированные контейнеры в среде выполнения

ОС хоста

- Большая площадь атак
- Общее ядро ОС для контейнеров
- Уязвимости компонентов ОС
- Некорректная настройка прав доступа
- Возможность доступа контейнеров к файловой системе

eBPF для изоляции приложений

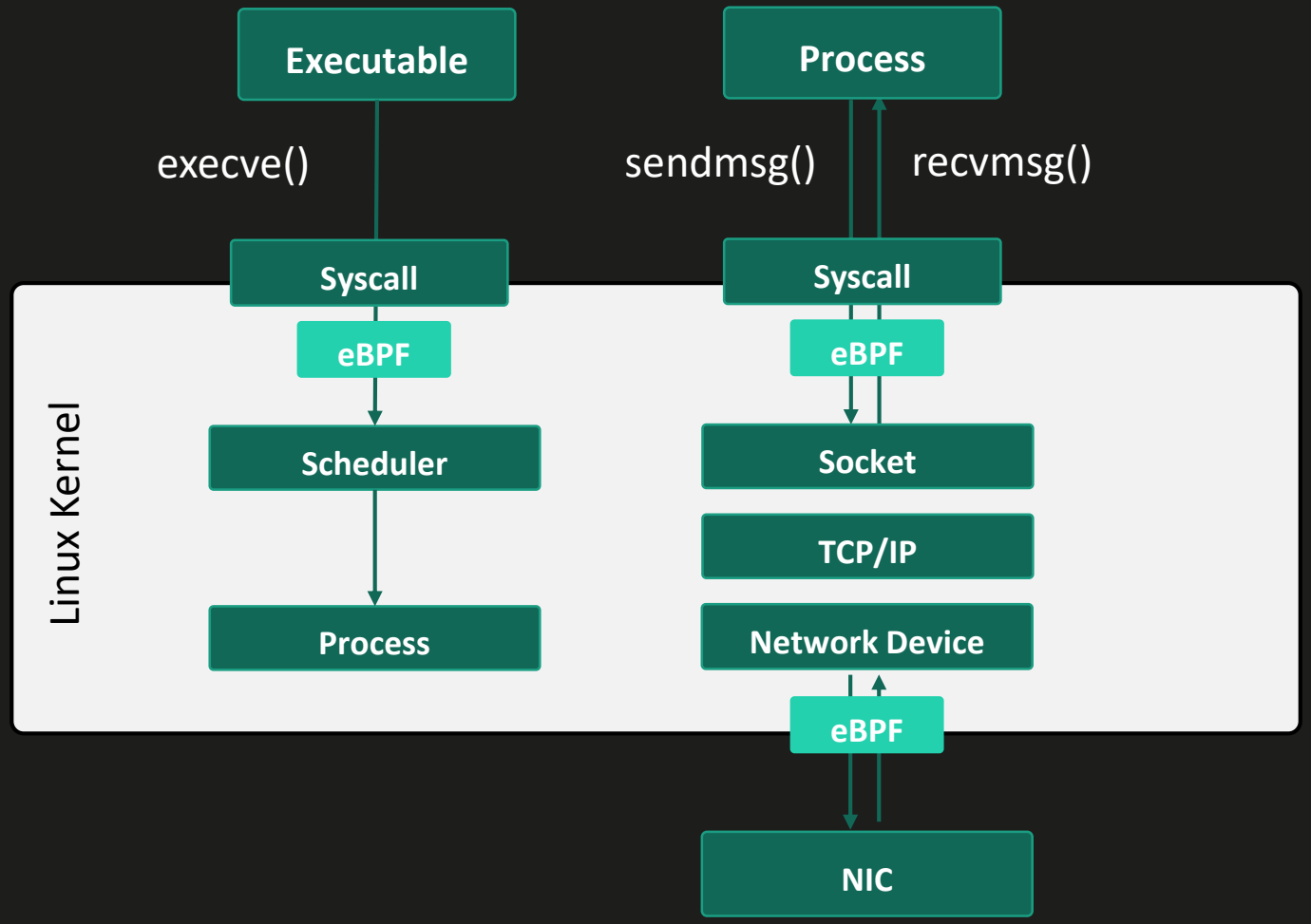


eBPF – “виртуальная машина” в ядре Linux

eBPF выполняет микропрограммы BPF, вызванные **триггерами на события** для целевых объектов ядра операционной системы

Позволяет контролировать практически любые системные операции (ограничено версией ядра операционной системы)

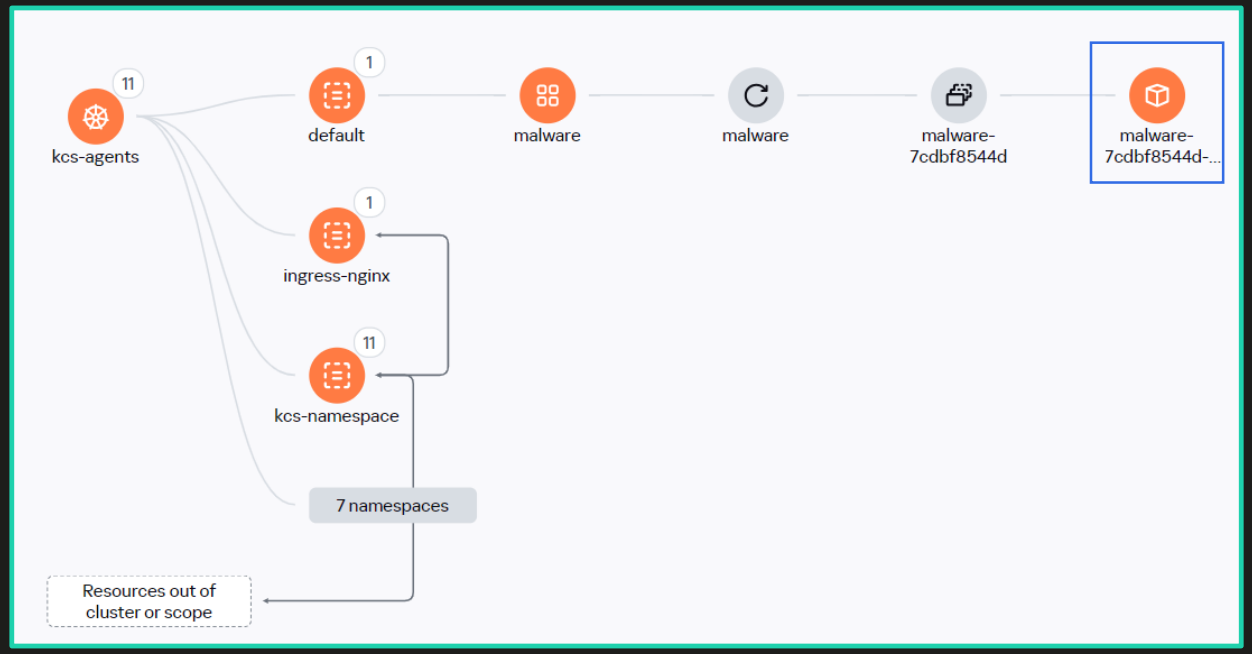
eBPF для изоляции приложений



Можно **изолировать приложение** в контейнере от нежелательных сетевых коммуникаций

Можно **запретить запуск** каких-либо **сторонних процессов** внутри контейнера (не дать атакующему развить атаку)

eBPF для статистики

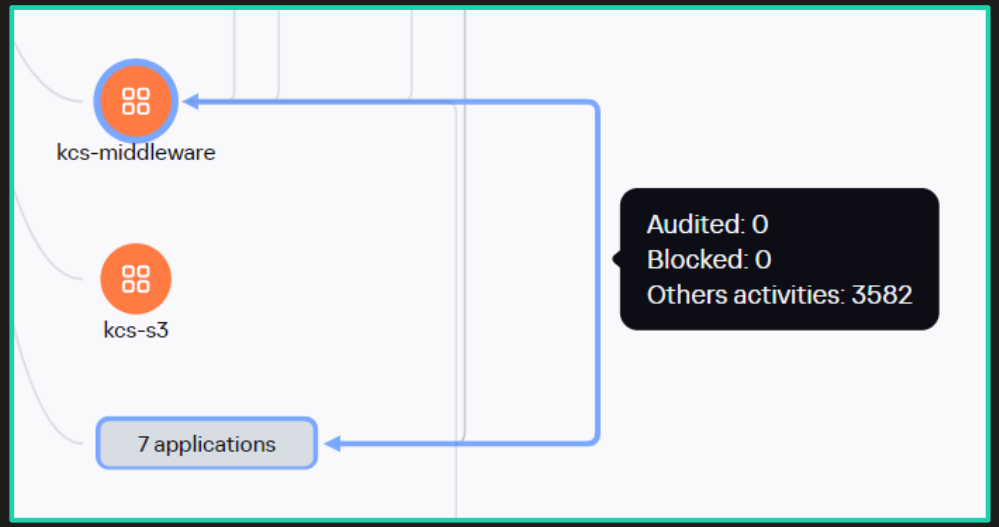


Network activity

Data for the last 15 min.

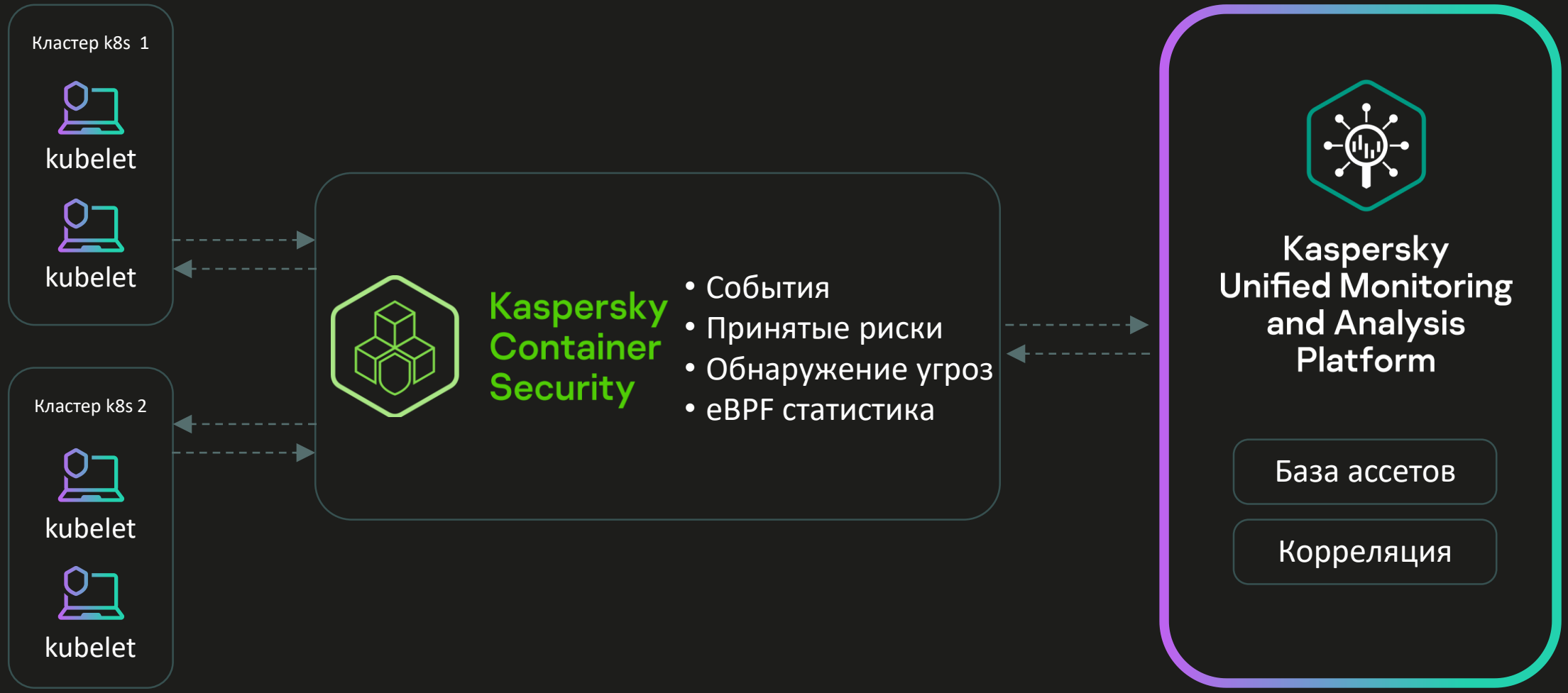
Audited activity 58 | Blocked activity | Others

Source	Protocol	Destination	Number of connections	Last connection
malware-7cdbf8544d-tbmkz 10.1.126.8:45782	TCP	lb-in-f101.1e100.net. 142.251.1.101:443	13	5/22/2024, 13:53:57
malware-7cdbf8544d-tbmkz 10.1.126.8:37012	TCP	lt-in-f99.1e100.net. 108.177.14.99:443	15	5/22/2024, 13:53:57
lb-in-f101.1e100.net. 142.251.1.101:443	TCP	malware-7cdbf8544d-tbmkz 10.1.126.8:45782	12	5/22/2024, 13:53:57
lt-in-f99.1e100.net. 108.177.14.99:443	TCP	malware-7cdbf8544d-tbmkz 10.1.126.8:37012	18	5/22/2024, 13:53:57



Детали сетевой активности

Регистрация событий на KUMA



Kaspersky Container Security

Kaspersky Unified Monitoring & Analysis