Профилирование и защита современных приложений

Рыбалко Алексей Алексеевич
alexey.rybalko@kaspersky.com

13.03.2024

План

- Уязвимости приложений в запущенном состоянии
- Состав контейнера
- Цифровая подпись на контейнере
- Анализ запросов с eBPF
- Сбор и анализ событий
- Инструменты защиты – Open Source
- Инструменты защиты – Enterprise

Основные риски ключевых компонентов контейнерных сред

Образы

Открытые внешние источники

Уязвимости ПО

Ошибки в конфигурациях

Вредоносное ПО

Секреты в открытом виде

Использование недоверенных образов

Реестр образов

Незащищенное подключение

Наличие устаревших образов с уязвимостями и вредоносным ПО

Недостаточные ограничения на аутентификацию и авторизацию

Оркестратор

Не ограничен административный доступ

Доступ без авторизации

Отсутствует или слабое разделение трафика между контейнерами

Не разнесены по хостам контейнеры с разным уровнями защиты данных

Ошибки в конфигурации оркестратора

Контейнеры

Уязвимости среды выполнения

Неограниченный доступ контейнеров к сети

Небезопасные конфигурации

Уязвимости приложений в контейнерах

Незапланированные контейнеры в среде выполнения

ОС хоста

Большая площадь атак

Общее ядро ОС для всех контейнеров

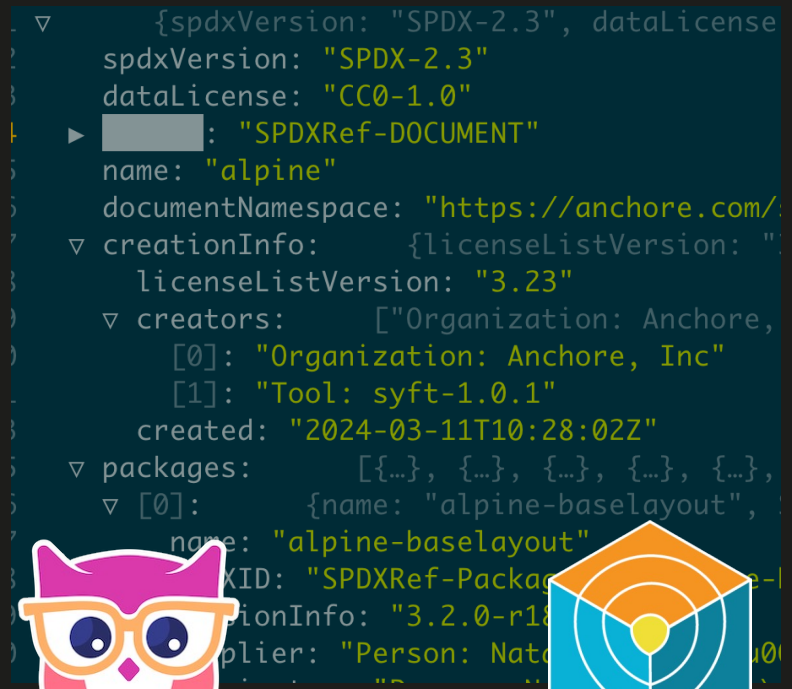
Уязвимости компонентов ОС

Некорректная настройка прав доступа пользователей

Возможность доступа контейнеров к файловой системе

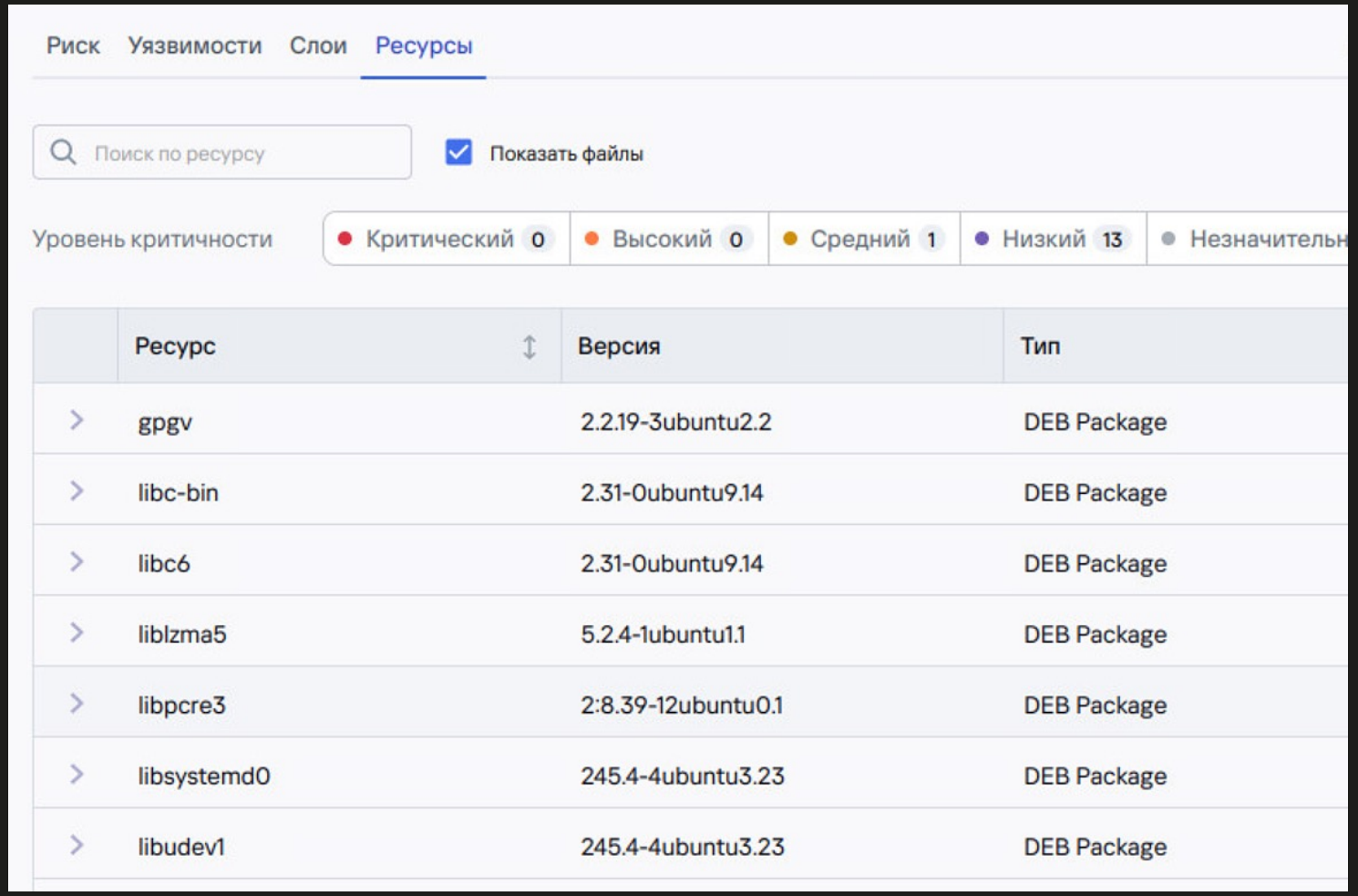
Software Bill of Materials

- Слои контейнеров
- Зависимости
- Уязвимости



syft

trivy

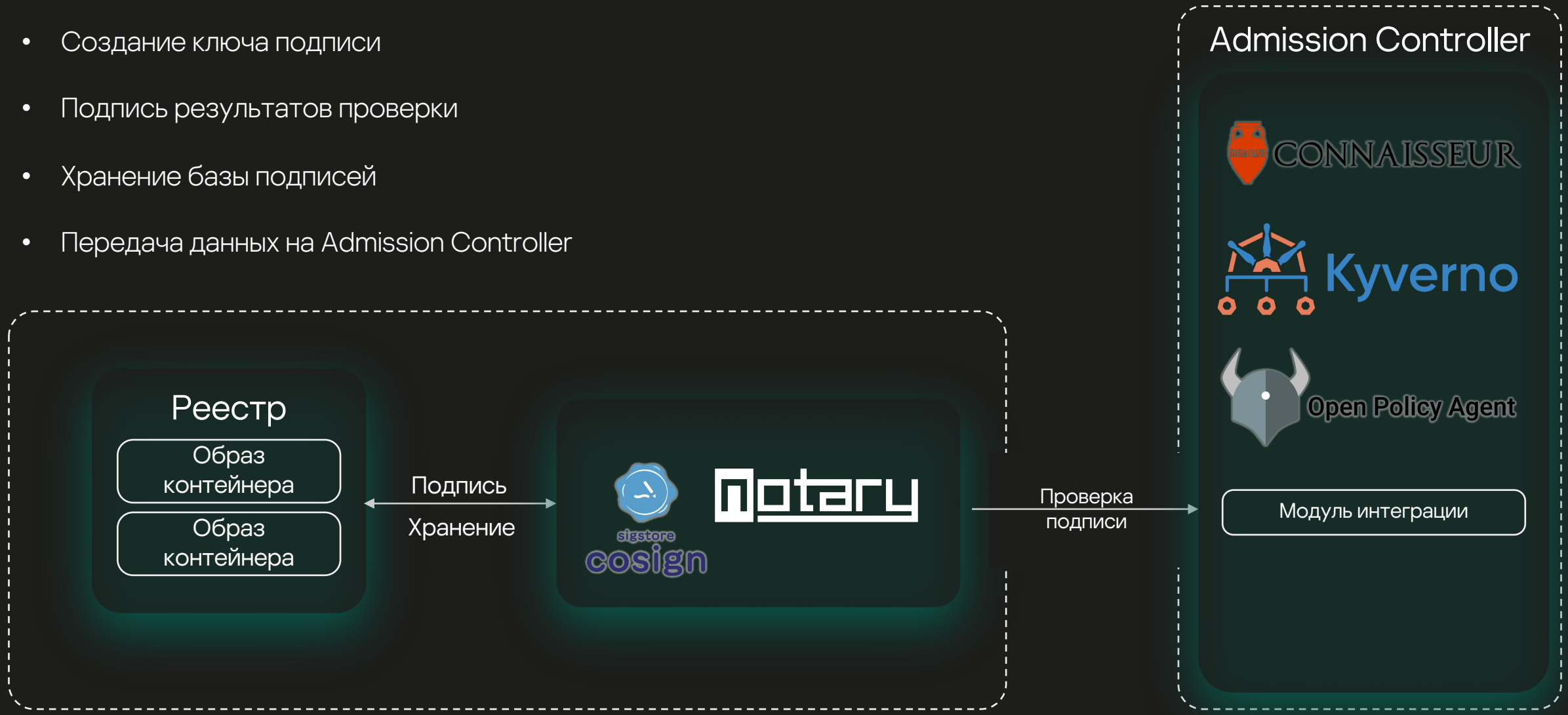


CycloneDX

SPDX

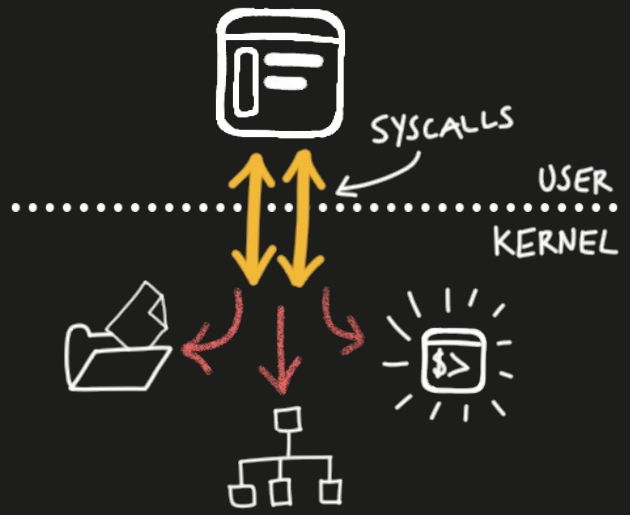
Подпись результата сборки

- Создание ключа подписи
- Подпись результатов проверки
- Хранение базы подписей
- Передача данных на Admission Controller



Анализ запросов к ядру

- Фильтрация запросов к ядру:
  - execv()
  - сетевые соединения
- Формирование профиля контейнера
- Контроль по принципу Service Mesh: sidecar container в каждом Pod
- Контроль с помощью центрального ядра Worker Node: фильтрация eBPF



Falco

tetragon

Запуск и реализация процессов из указанных исполняемых файлов запрещаются, кроме процессов из файлов-исключений.

Блокировать запуск всех исполняемых файлов

Блокировать указанные исполняемые файлы

Путь к исполняемым файлам или директориям *

Укажите путь к конкретным бинарным исполняемым файлам или директориям. Используйте маску /*, чтобы распространить блокирование на всю директорию и ее поддиректории. Вы можете ввести только название программы без определения пути, чтобы заблокировать ее запуск по всем путям.

Разрешить исключения

Путь к исполняемым файлам или директориям *

/bin/dash /usr/bin/which /usr/local/sbin/haproxy-systemd-wrapper /usr/local/sbin/haproxy /bin/busybox

Укажите путь к конкретным бинарным исполняемым файлам или директориям. Используйте маску /*, чтобы разрешить запуск из этой директории и ее поддиректорий. Вы можете ввести только название программы без определения пути, чтобы разрешить ее запуск по всем путям.

Ограничение входящих сетевых соединений Выключено

Все источники сетевых соединений блокируются, кроме указанных как исключения.

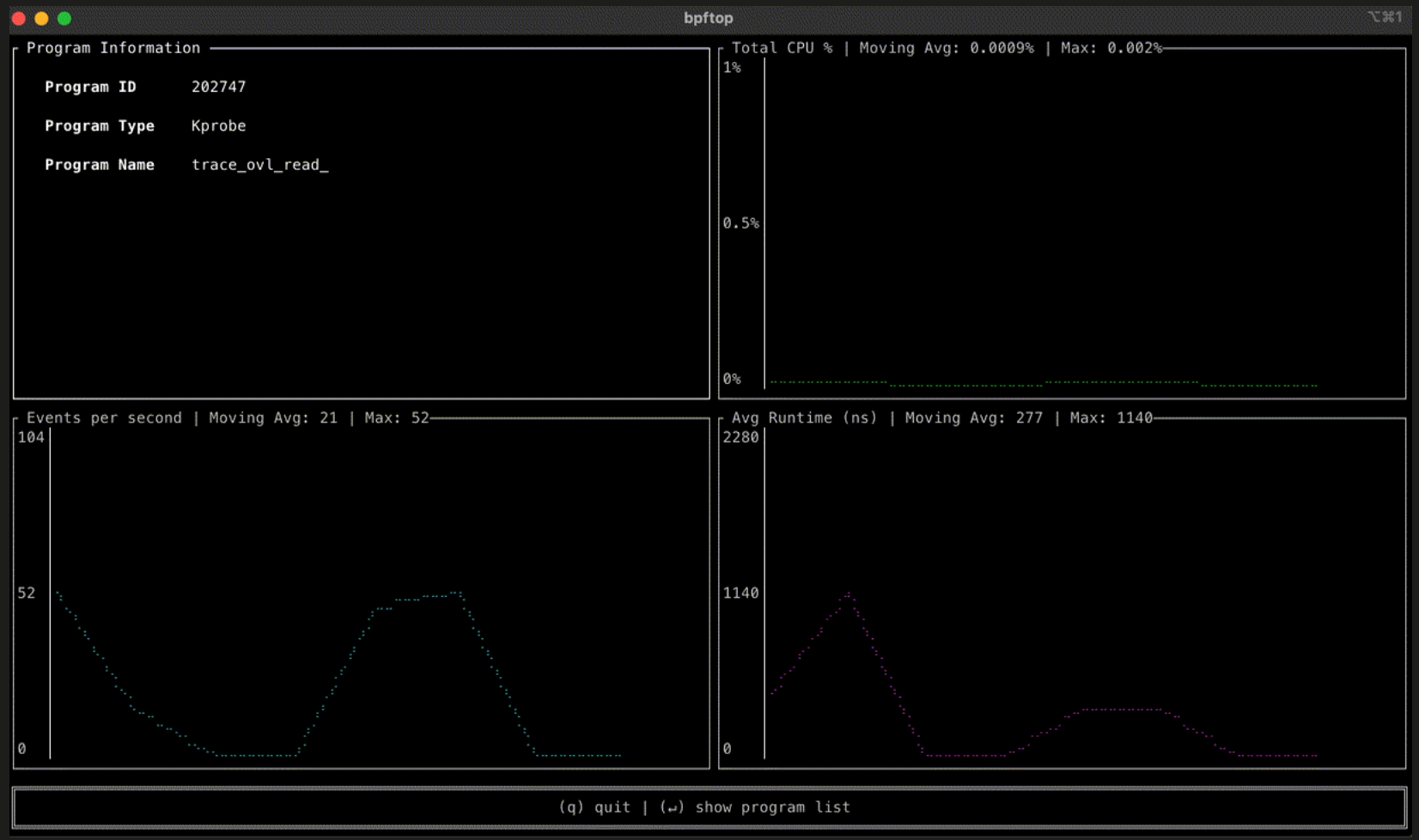
Ограничение исходящих сетевых соединений Выключено

Все точки назначения сетевых соединений блокируются, кроме указанных как исключения.

Производительность vs надёжность фильтрации eBPF

- Упреждающая проверка процесса
- Проверка по факту запуска и выполнения действий
- Контроль производительности программ BPF

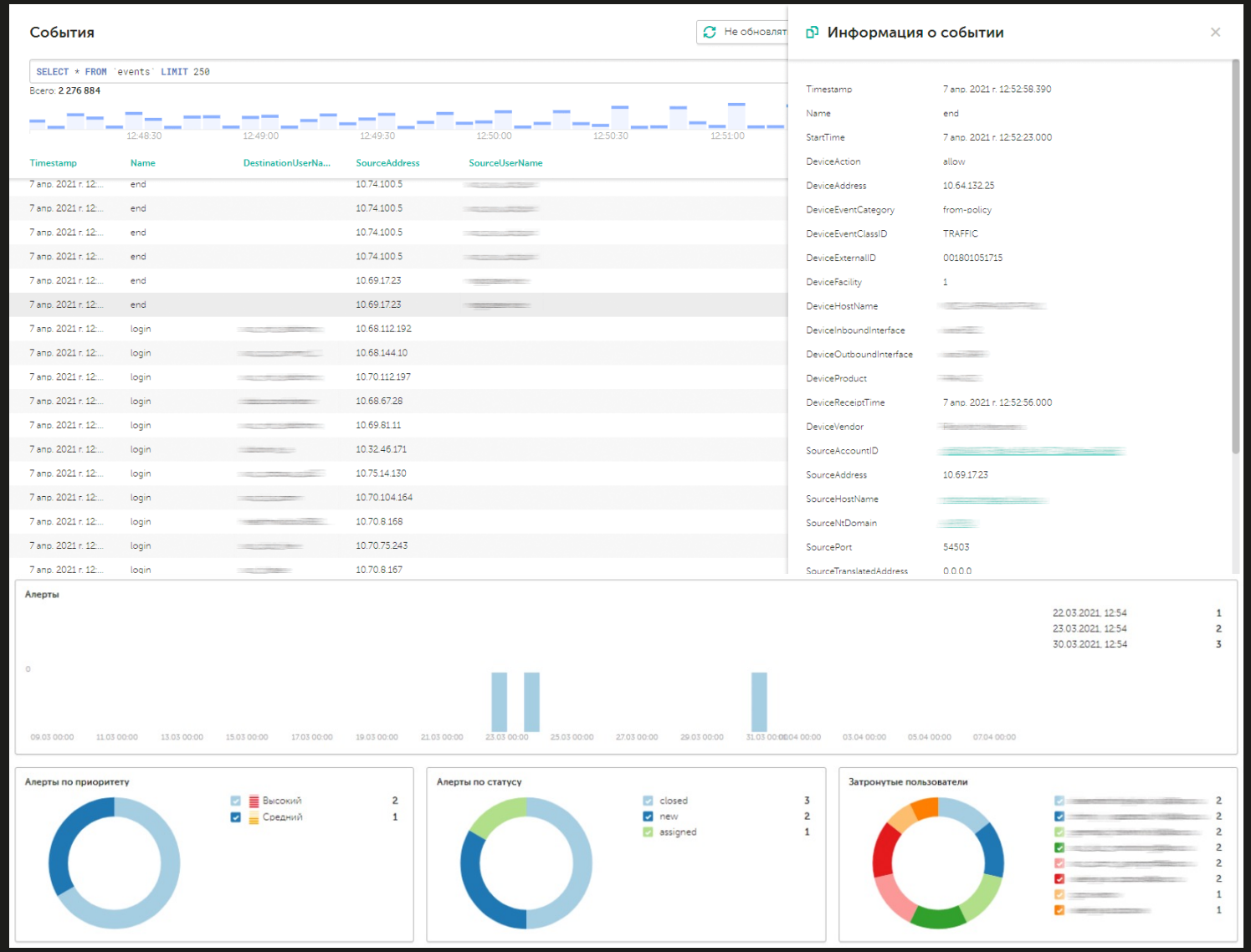
bpftop



INSPEKTOR GADGET

Аудит и сбор событий

- Сбор событий о работе приложений в runtime
- Передача событий по протоколу syslog на внешнюю SIEM (SOC)
- Заведение инцидентов по факту срабатывания программ eBPF



logstash

Grafana loki

Инструментарий Open Source для контейнеров (CNCF)

Архитектура Kaspersky Container Security (KCS)

Ссылки

- NIST Special Publication 800-190 - https://doi.org/10.6028/NIST.SP.800-190
- Anchore Syft - https://github.com/anchore/syft
- Aqua Security Trivy - https://github.com/aquasecurity/trivy
- Sigstore Cosign - https://github.com/sigstore/cosign
- Notary Project - https://github.com/notaryproject
- Подробная статья об Extended BPF - https://habr.com/ru/articles/514736/
- Falco - https://github.com/falcosecurity/falco
- Cilium Tetragon - https://tetragon.io/docs/
- Netflix bpftop - https://github.com/Netflix/bpftop
- Inspektor Gadget - https://github.com/inspektor-gadget/inspektor-gadget
- Cloud Native Landscape - https://landscape.cncf.io/
- Logstash - https://www.elastic.co/logstash
- Grafana Loki - https://github.com/grafana/loki
- Kaspersky Container Security - https://www.kaspersky.com/enterprise-security/container-security

Спасибо!