Иван Соломатин

Руководитель направления
защиты приложений

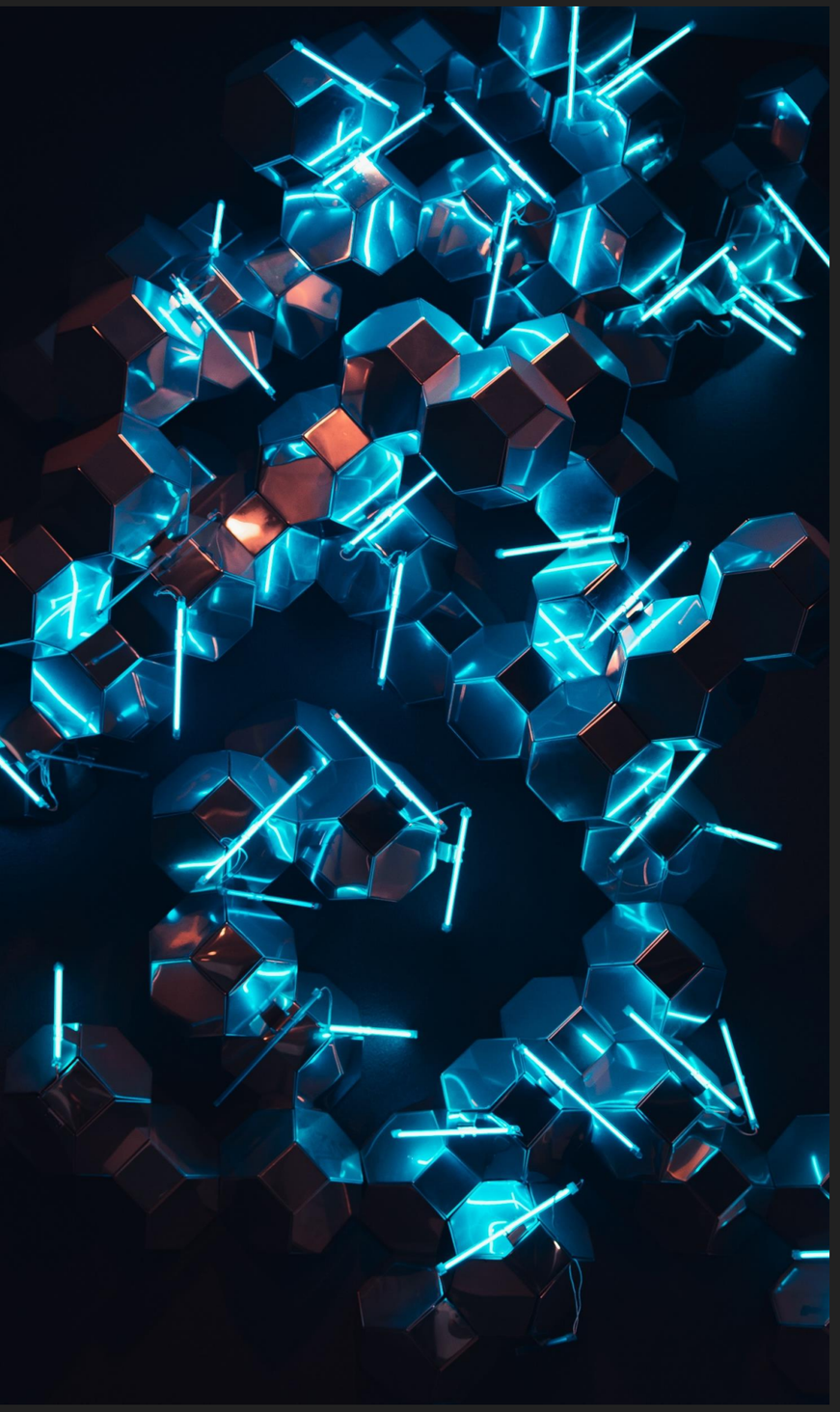
Тренды безопасности в разработке: от $ до ;

О спикере

- Более 5 лет занимаюсь направлением AppSec
- Активный участник IT\Sec community от бизнеса
- Отвечаю за технологический и коммерческий успех продуктового направления в Positive Technologies
- Первый раз в Самаре ☺

- isolomatin@ptsecurity.com
- TG: @soulmatin

Добавляйтесь на LinkedIn



Обсудим следующее:

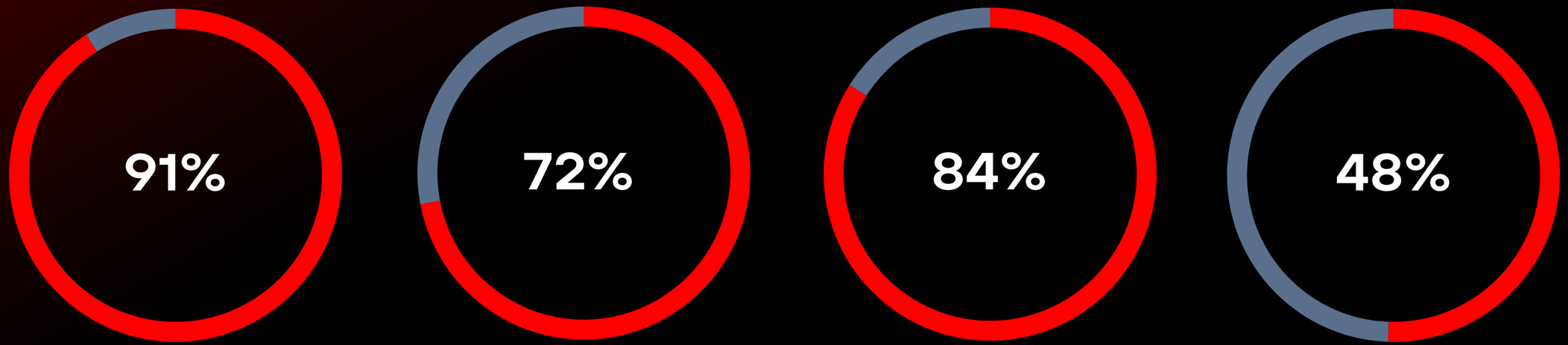
- Продолжим говорить про AppSec
- Посмотрим аналитику по уязвимостям
- Positive Technologies тоже важно защищать приложения
- Разберём тренды

Пенсионер, который освоил Rust

- Удалёнка
- Высокий доход
- Престижная профессия
- Очередь из офферов
- Интересные проекты

Текущее состояние защищенности

На примере веб-приложений*



Подвержены утечкам важных данных

Уязвимостей связаны с ошибками в коде

Предоставляют возможности несанкционированного доступа

Имеют низкий или крайне низкий уровень защищенности

По данным исследования Positive Technologies «Итоги пентестов — 2022», уязвимости веб-приложений стали причиной 86% случаев проникновения в сеть компании

Статистика говорит за себя

За 10 месяцев 2023 г. в мире было обнаружено больше уязвимостей, чем за весь 2022 г.

По данным Национальной базы данных уязвимостей (NVD), в октябре 2023 г. было зарегистрировано 25 356 уязвимостей, что превышает общий показатель за весь предыдущий год (25 051 уязвимость). Рост количества уязвимостей является частью тренда, начавшегося в 2018 г. и не прекращающегося по сегодняшний день. Такая динамика подчеркивает критическую важность оперативного обнаружения и исправления уязвимостей разработчиками ПО для предотвращения их эксплуатации киберпреступниками.

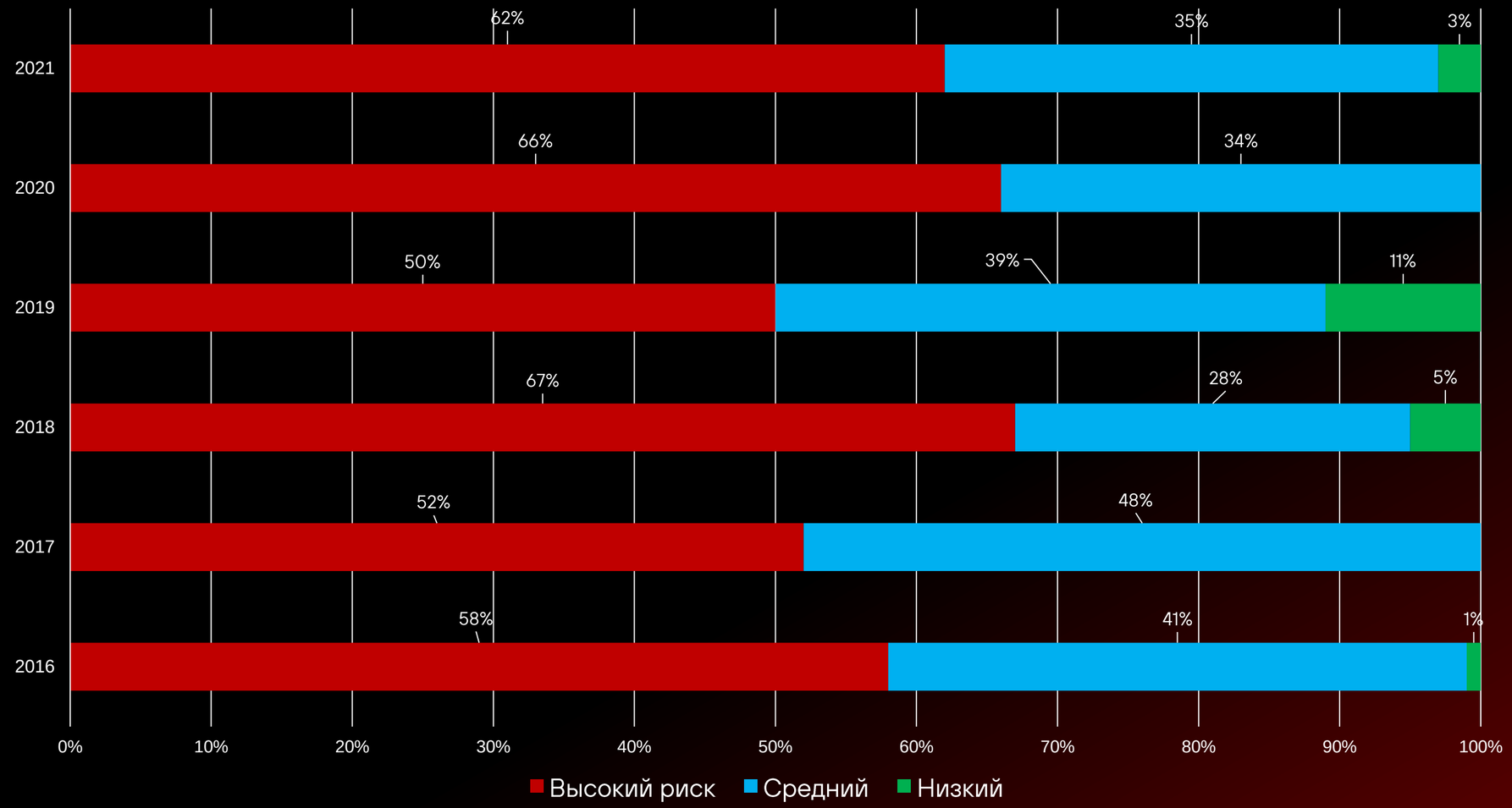
* Исследование Positive Technologies за 2023 год

Уязвимости — это не то, на что можно закрыть глаза

72% уязвимостей содержатся в коде приложения

15 уязвимостей в среднем имеет каждое приложение

Каждая седьмая уязвимость высокого уровня риска



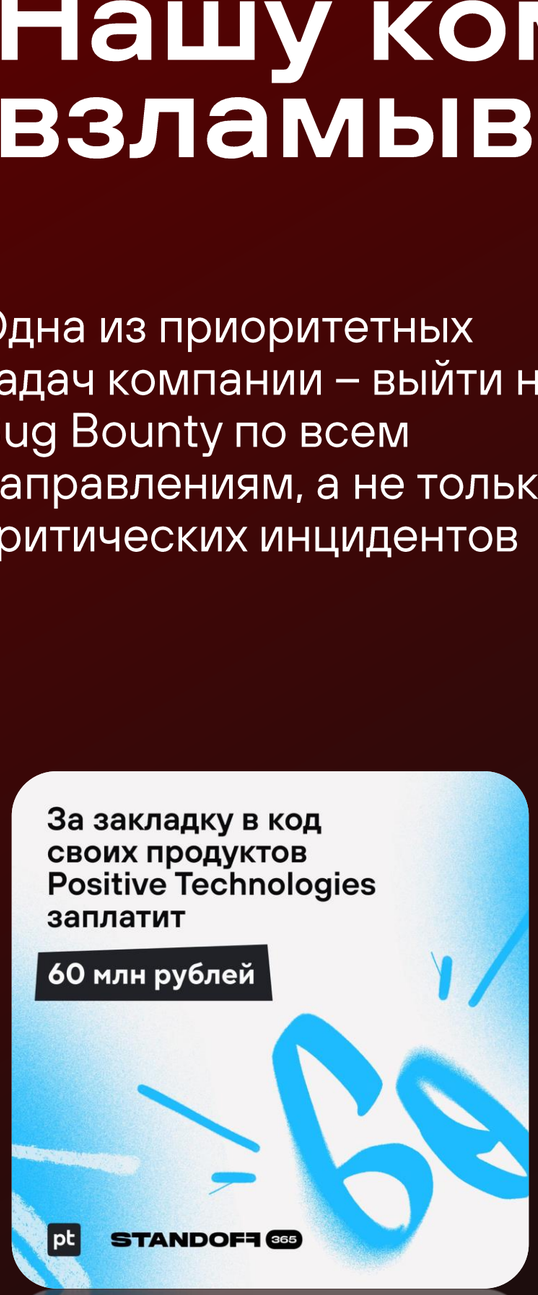
Уязвимости и угрозы веб-приложений 2020-2021 г.г., Positive Technologies

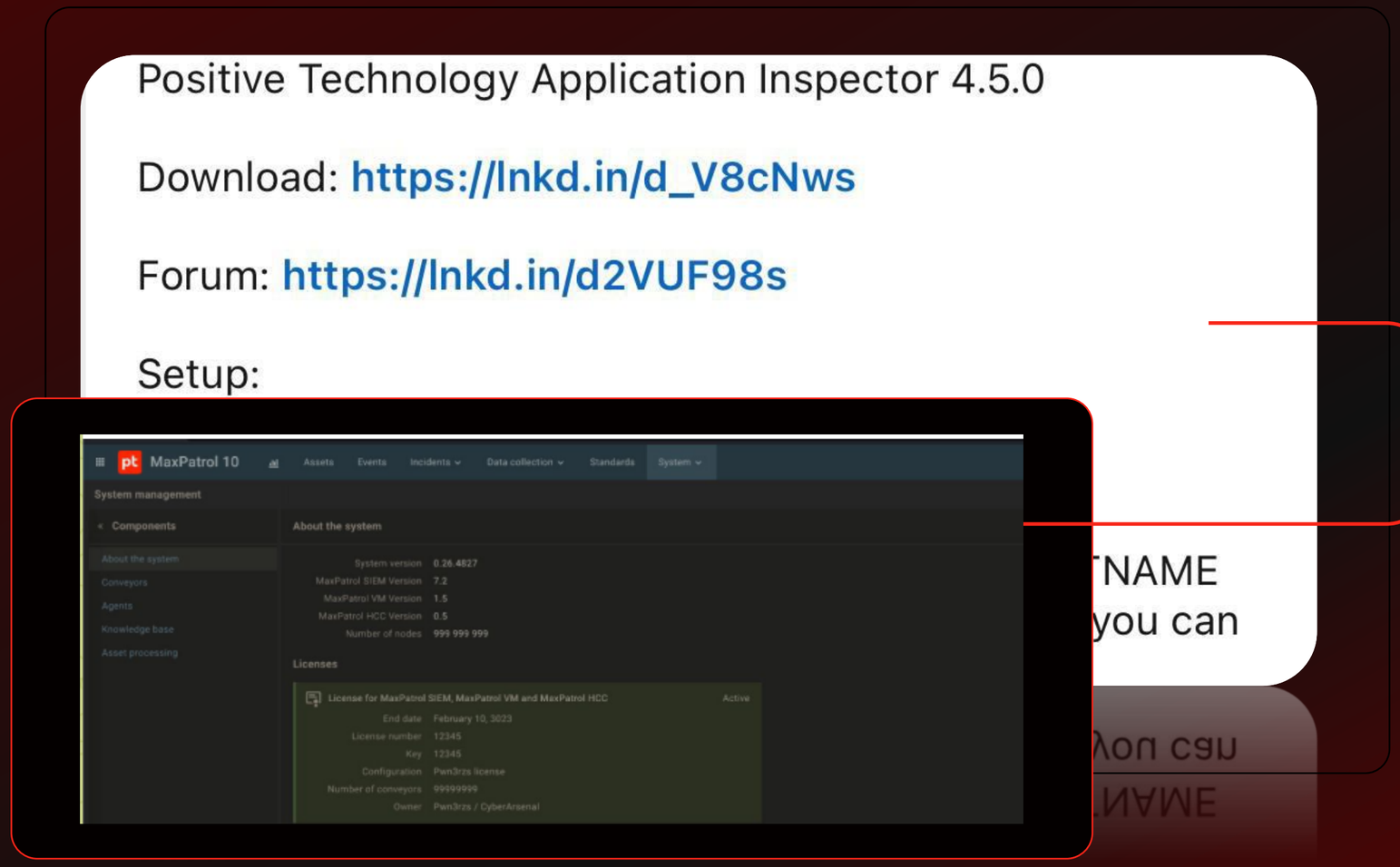
Последствия взлома приложений

- Получение доступа к сети
- Кража данных клиентов
- Атака на ваших клиентов
- Потеря денег
- Удар по репутации
- Иные юридические риски

Нашу компанию тоже пытаются взламывать

Одна из приоритетных задач компании – выйти на Bug Bounty по всем направлениям, а не только критических инцидентов





Как говаривал народ – «Если ваш продукт появился на torrent, значит он востребован и выполняет свои функции»

Какое же направление?

Особенности современной разработки

- Большие объемы кода
- Разнообразие языков и технологий
- Массовость при одновременном дефиците квалифицированных кадров
- Повсеместное использование сторонних компонентов
- Высочайшие темпы для снижения Time-To-Market
- Общая недооценка темы ИБ применительно к R&D

В этой ситуации появление уязвимостей в коде видится неизбежным. Для того, чтобы вовремя их выявлять и устранять, необходимо проводить анализ программного кода на уязвимости

Блокчейн

- Блокчейн за пределами криптовалют – это уже случившийся факт
- Рост числа мобильных приложений приводит к увеличению числа приложений на основе блокчейна.
- Децентрализованные приложения (DApps) построены на технологии blockchain
- Синтаксис языка Solidity схож с JavaScript и Python - доступен и понятен

След безопасности в разработке

- Интеграция передовых протоколов безопасности и использование искусственного интеллекта для обнаружения угроз.
- Акцент на DevSecOps. Компании интегрируют безопасность в свои процессы DevOps,
- Архитектура Zero Trust. Принцип «никогда не доверяй, всегда проверяй».
- Более широкое использование шифрования.
- Фокус на практике безопасного кода.
- Расцвет сети кибербезопасности (cybersecurity mesh).

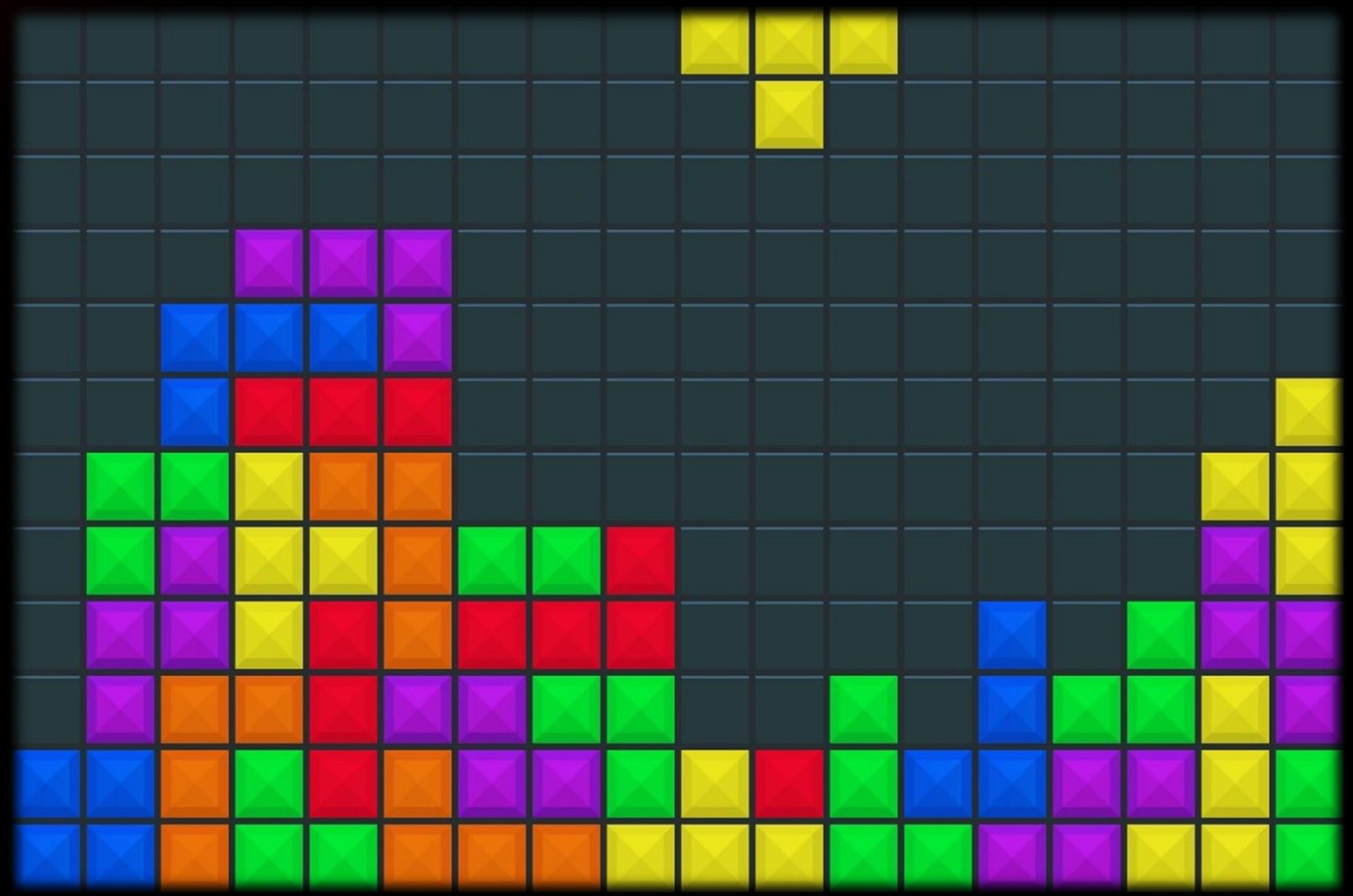
Интеграция искусственного интеллекта и машинного обучения

- Технологии AI/ML: от алгоритмов прогнозирования до автоматизированных проверок кода

- Разработчики стали чаще использовать инструменты искусственного интеллекта при написании кода

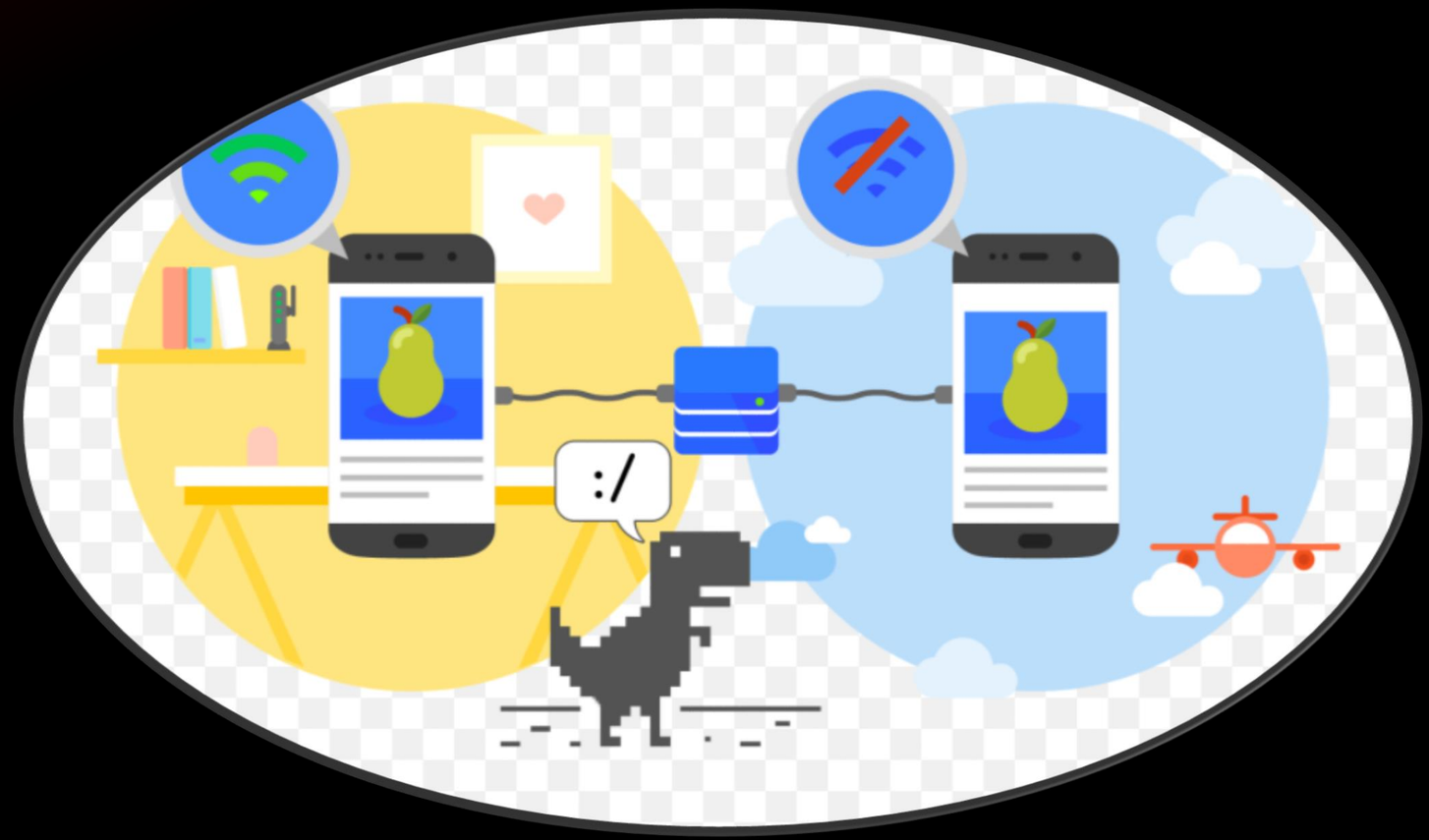
Множественность микросервисов

- Микросервисы с множественными средами выполнения (multi-runtime microservices)
- Приложения в собственной среде исполнения
- Командная работа над разными сервисами без зависимостей



Рост числа прогрессивных веб-приложений (PWA)

- PWA (Progressive Web Apps) требуют меньше ресурсов, чем нативные приложения
- Быстрая загрузка
- Работают в автономном режиме и автоматически обновляются при каждом посещении
- Экономичны и эффективны
- Независимость от платформы
- Быстрая разработка и дешевая поддержка



Безопасность разработчику

- Эффективность разработки включает в себя не только навыки программиста, но и рабочее окружение. Плагины/расширения IDE помогают оптимизировать процесс

- Плагины для безопасной разработки находят уязвимости и не задокументированные возможности в коде приложения, в процессе его написания. Встроенные модули анализа обнаруживают уязвимости исходного кода и ошибки конфигурационных файлов, используемые в процессе разработки

Будьте в курсе событий

POSIDEV

Канал PT AF

Канал PT CS

Канал PT AI

pt@ptsecurity.com

ptsecurity.com

Спасибо!