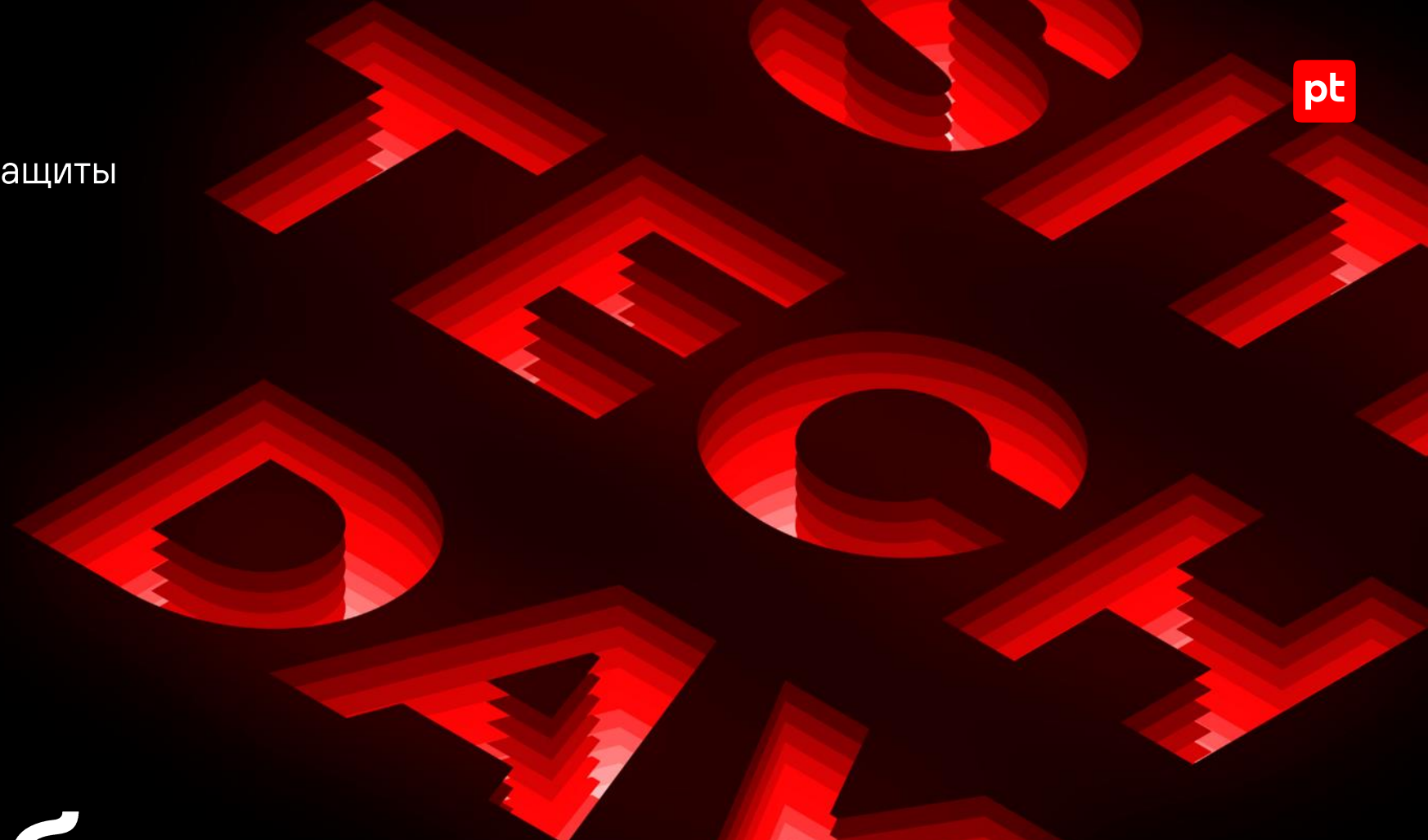
Иван Соломатин

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 Новосибирске ☺

Добавляйтесь в LinkedIn

isolomatin@ptsecurity.com

@soulmatin

Что обсудим

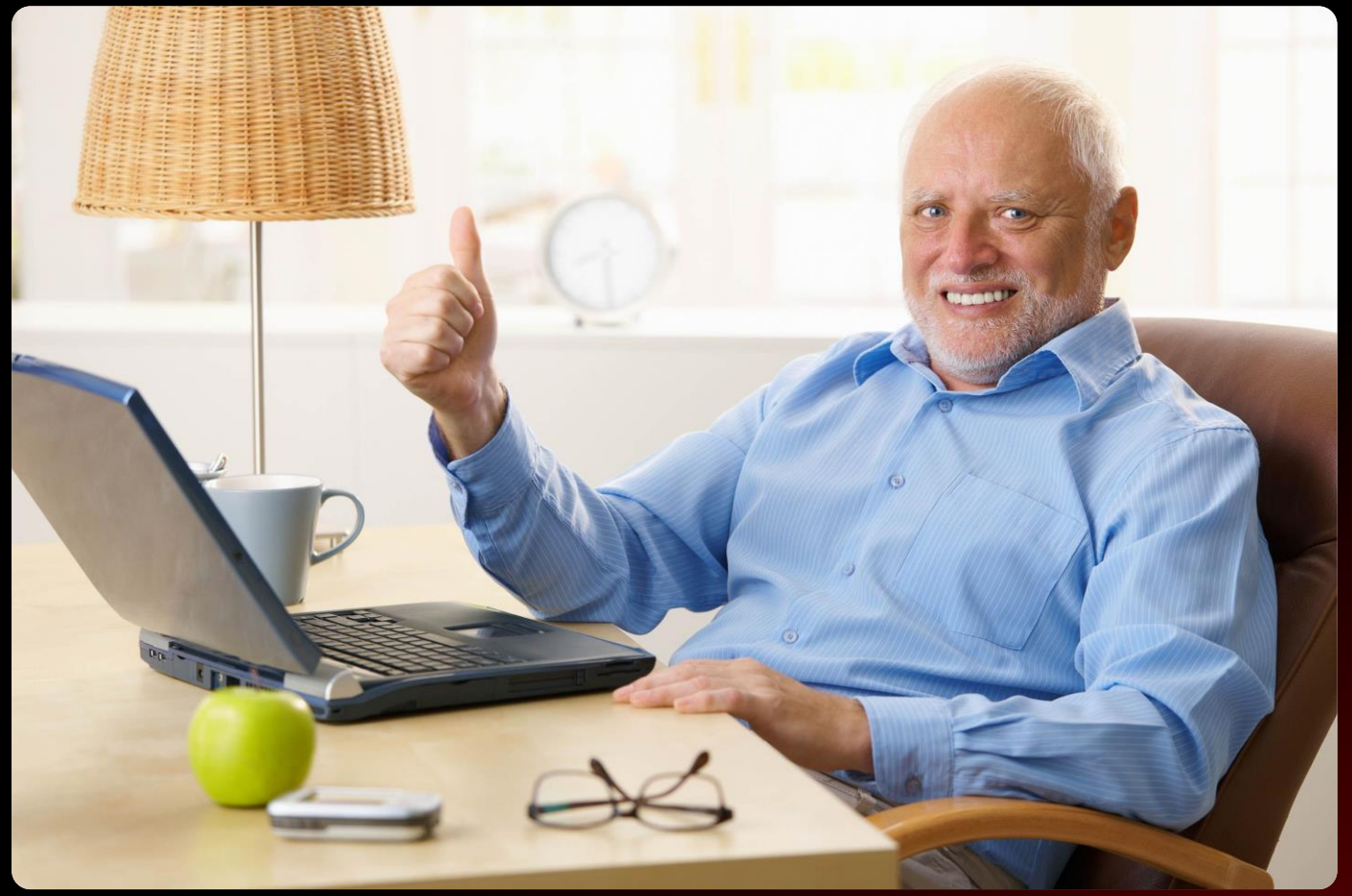
- Продолжим говорить про AppSec
- Посмотрим аналитику по уязвимостям
- Positive Technologies тоже важно защищать приложения
- Разберем тренды

Пенсионер, который освоил Rust

pt

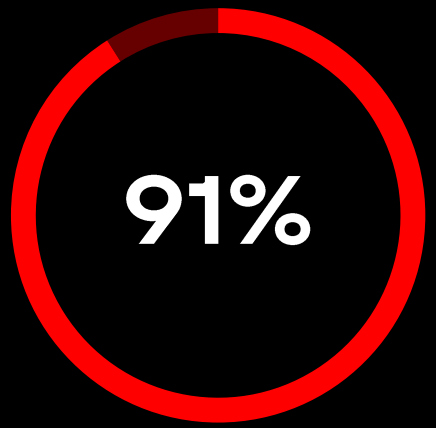
>

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

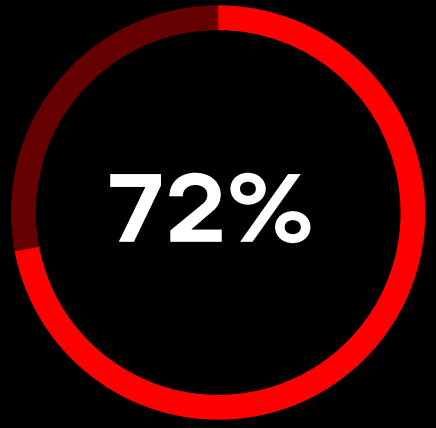


Текущее состояние защищенности

На примере веб-приложений*

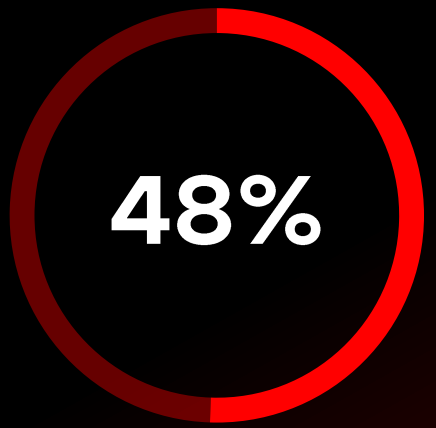


Подвержены утечкам важных данных



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 года в мире было обнаружено больше уязвимостей, чем за весь 2022 год.
По данным Национальной базы данных уязвимостей (NVD), в октябре 2023 года было зарегистрировано 25 356 уязвимостей, что превышает общий показатель за весь предыдущий год (25 051 уязвимость). Рост количества уязвимостей — это часть тренда, начавшегося в 2018 году и не прекращающегося до сих пор. Такая динамика подчеркивает критическую важность оперативного обнаружения и исправления уязвимостей разработчиками ПО для предотвращения их эксплуатации киберпреступниками.

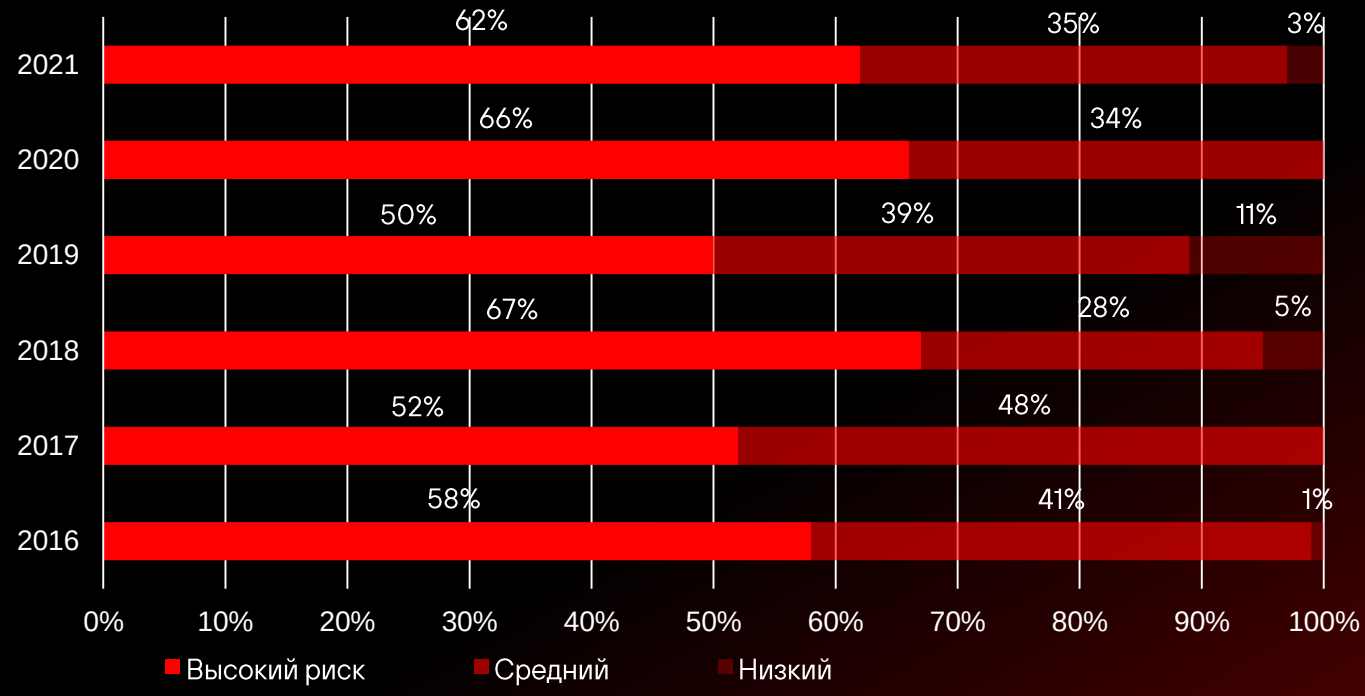
* Исследование Positive Technologies за 2023 год

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
имеет высокий уровень риска



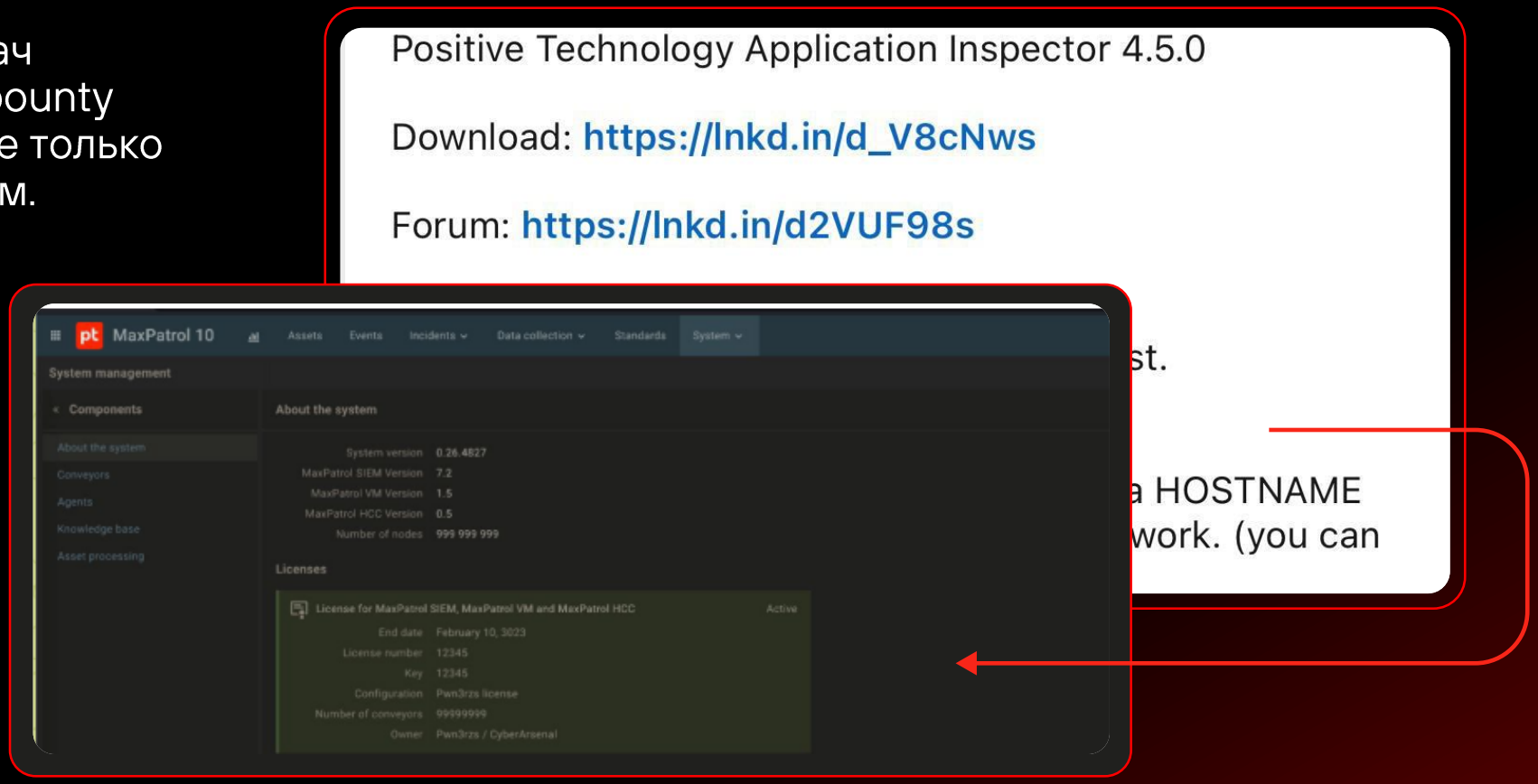
Уязвимости и угрозы веб-приложений в 2020–2021 годах, Positive Technologies

Последствия взлома приложений

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

Нашу компанию тоже пытаются взломать

Одна из приоритетных задач компании — выйти на bug bounty по всем направлениям, а не только по критическим инцидентам.



Как говорится, если ваш продукт появился на торрентах, 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. 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 блокчейна.
- Синтаксис языка Solidity схож с JavaScript и Python — доступен и понятен.

След безопасности в разработке

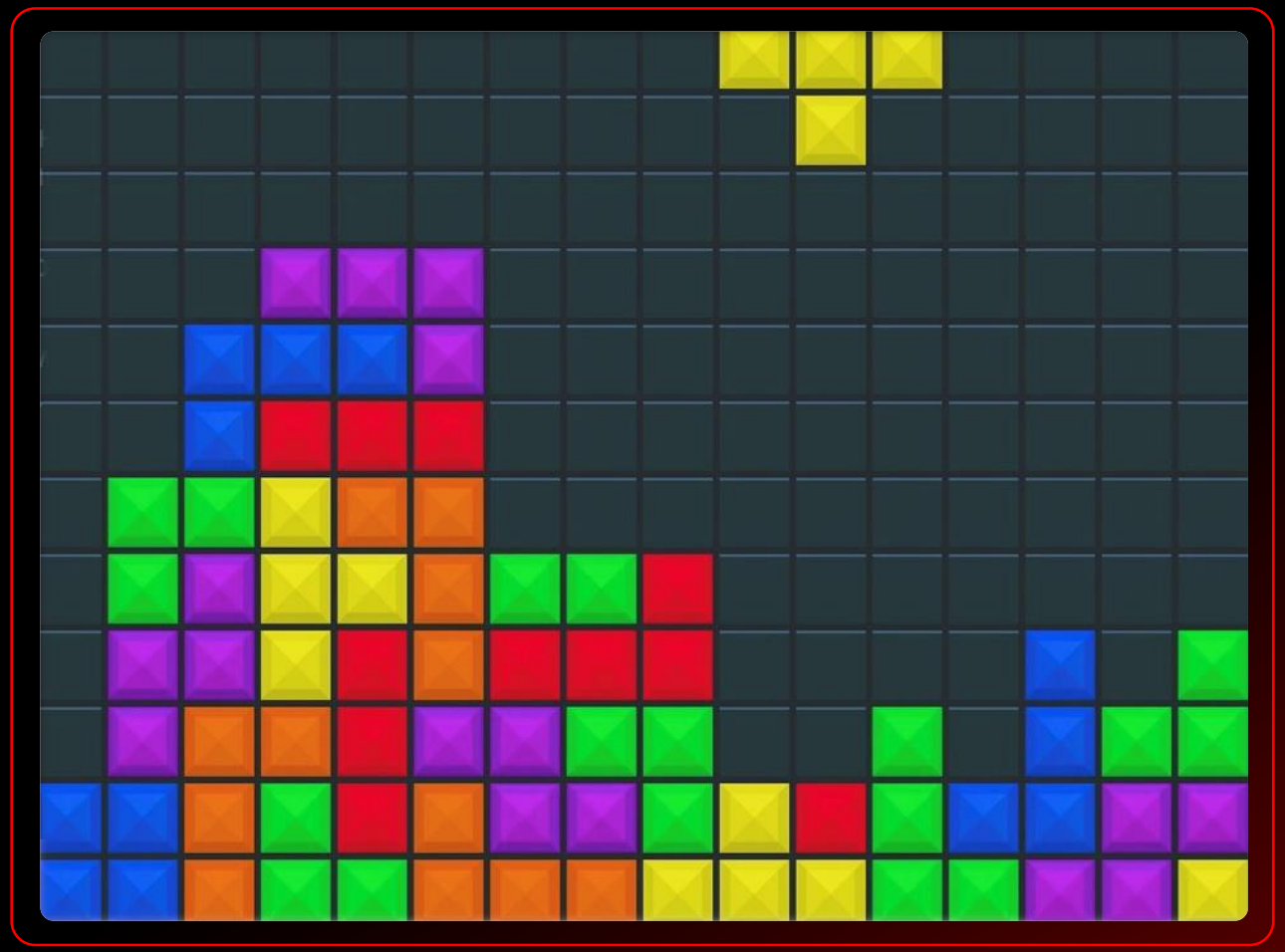
- Интеграция передовых протоколов безопасности и использование искусственного интеллекта для обнаружения угроз.
- Акцент на DevSecOps. Компании интегрируют безопасность в свои процессы DevOps.
- Архитектура zero trust. Принцип «никогда не доверяй, всегда проверяй».
- Более широкое использование шифрования.
- Фокус на практике безопасного кода.
- Расцвет сетей 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.

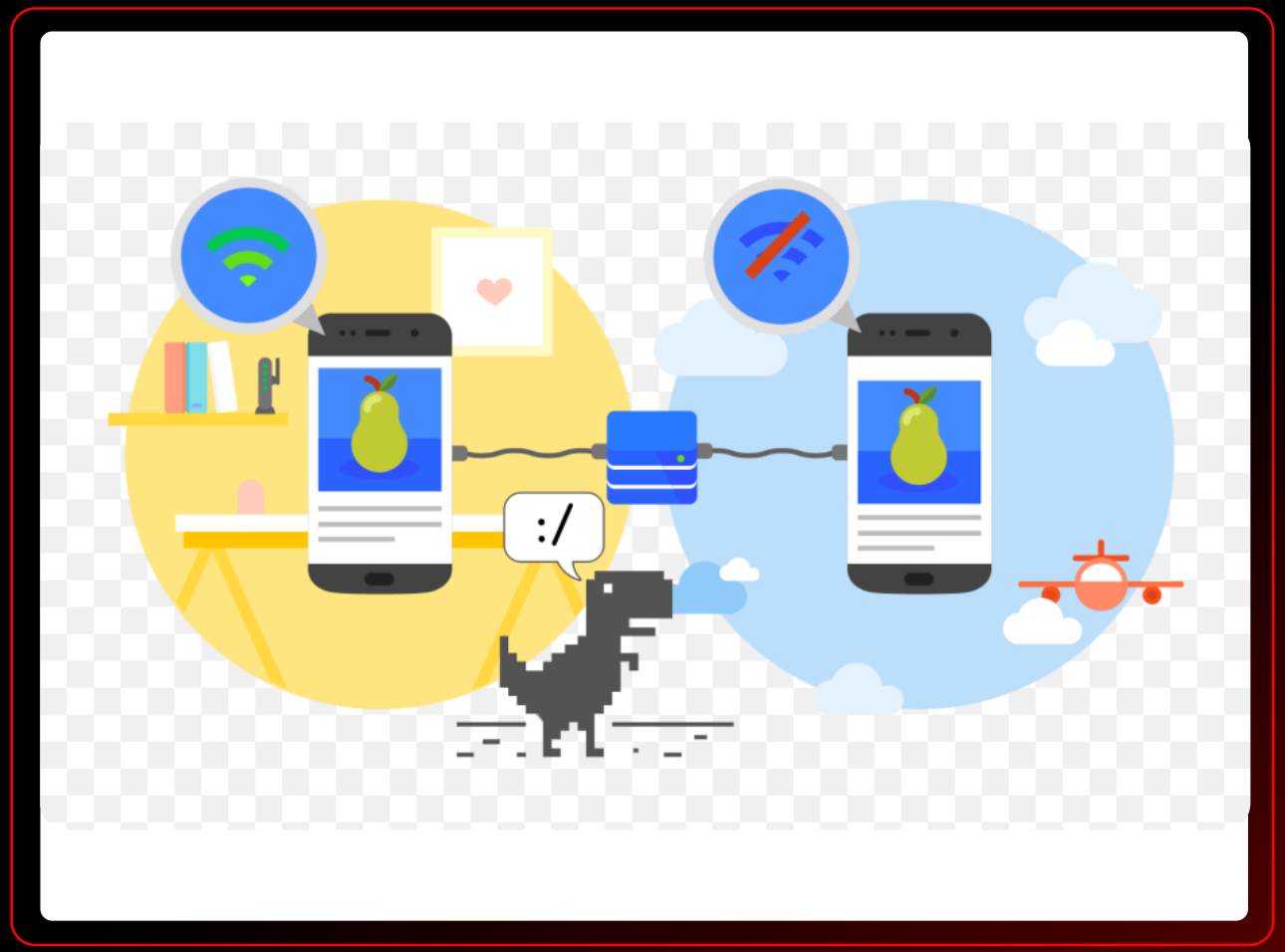
Множественность микросервисов

- 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.
- Быстро загружаются.
- Работают в автономном режиме и автоматически обновляются при каждом посещении.
- Экономичны и эффективны.
- Не зависят от платформы.
- Быстро разрабатываются и не требуют дорогой поддержки.



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 недокументированные возможности в коде приложения в процессе его написания. Встроенные модули анализа обнаруживают уязвимости исходного кода и ошибки конфигурационных файлов, используемых в процессе разработки.

Будьте в курсе событий

POSIdev

Канал PT AF

Канал PT CS

Канал PT AI

pt@ptsecurity.com

ptsecurity.com

Внимание, опрос!

Спасибо!