КРОК

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРАХОВАНИИ

Александр Черныхов
Эксперт по информационной безопасности

Андрей Крупнов
Директор по отраслевым решениям

ПОСТРОЕНИЕ ЦИФРОВОГО ВЗАИМОДЕЙСТВИЯ С ПОСРЕДНИКАМИ СТАНОВИТСЯ ОСНОВНОЙ ЗАДАЧЕЙ РАЗВИТИЯ ПРОДАЖ СТРАХОВАНИЯ

Посреднические
продажи е-ОСАГО

Предпочтение
посреднических каналов
продаж клиентами

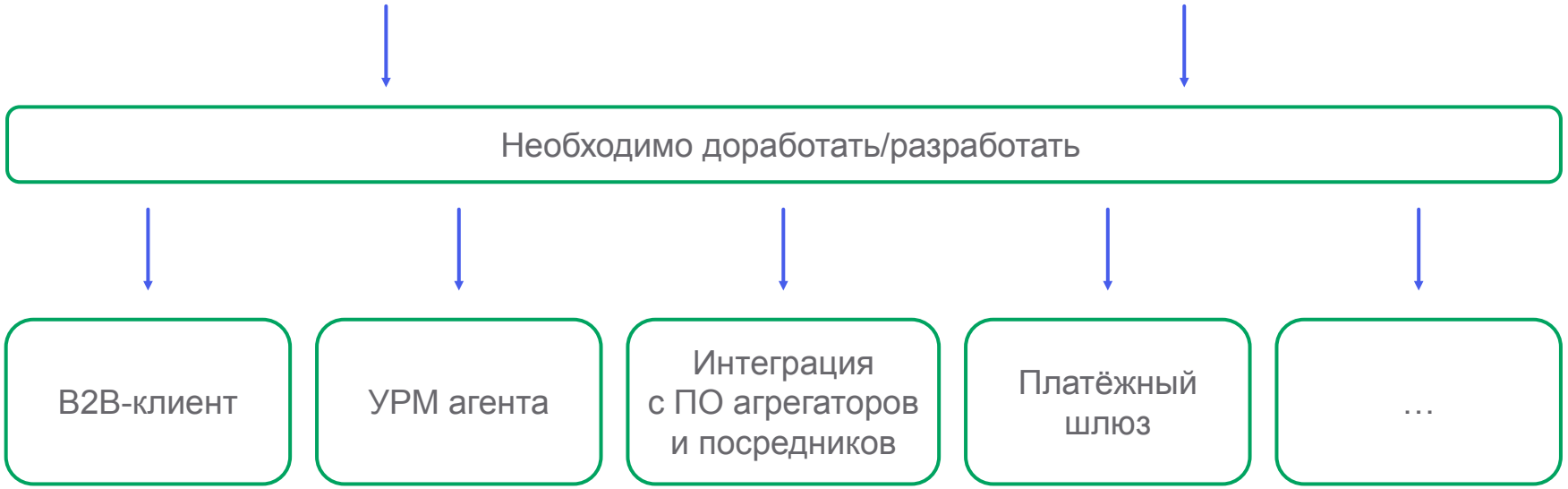
Массовый переход продаж страховых продуктов в цифровую форму (на стороне посредников)

КРОК

ОКОНЧАТЕЛЬНАЯ ЦИФРОВИЗАЦИЯ ПОСРЕДНИЧЕСКИХ ПРОДАЖ ПОТРЕБУЕТ ДОРАБОТКИ/РАЗРАБОТКИ ЦЕЛОГО КОМПЛЕКСА ИТ-СИСТЕМ

Агенты и брокеры будут действовать от имени страховщика. Платёж осуществляется непосредственно в пользу страховщика

Требуется наличие у посредника собственных программно-технических средств, позволяющих создавать и отправлять информацию в электронной форме в информационную систему страховщика



КРОК

НЕМНОГО СТАТИСТИКИ

Все приложения
содержат уязвимости[1]

В 65% случаев
Возможно получение полного контроля над всеми данными организации[1]

В 72% случаев
Возможно вторжение за периметр организации через веб-уязвимости[1]

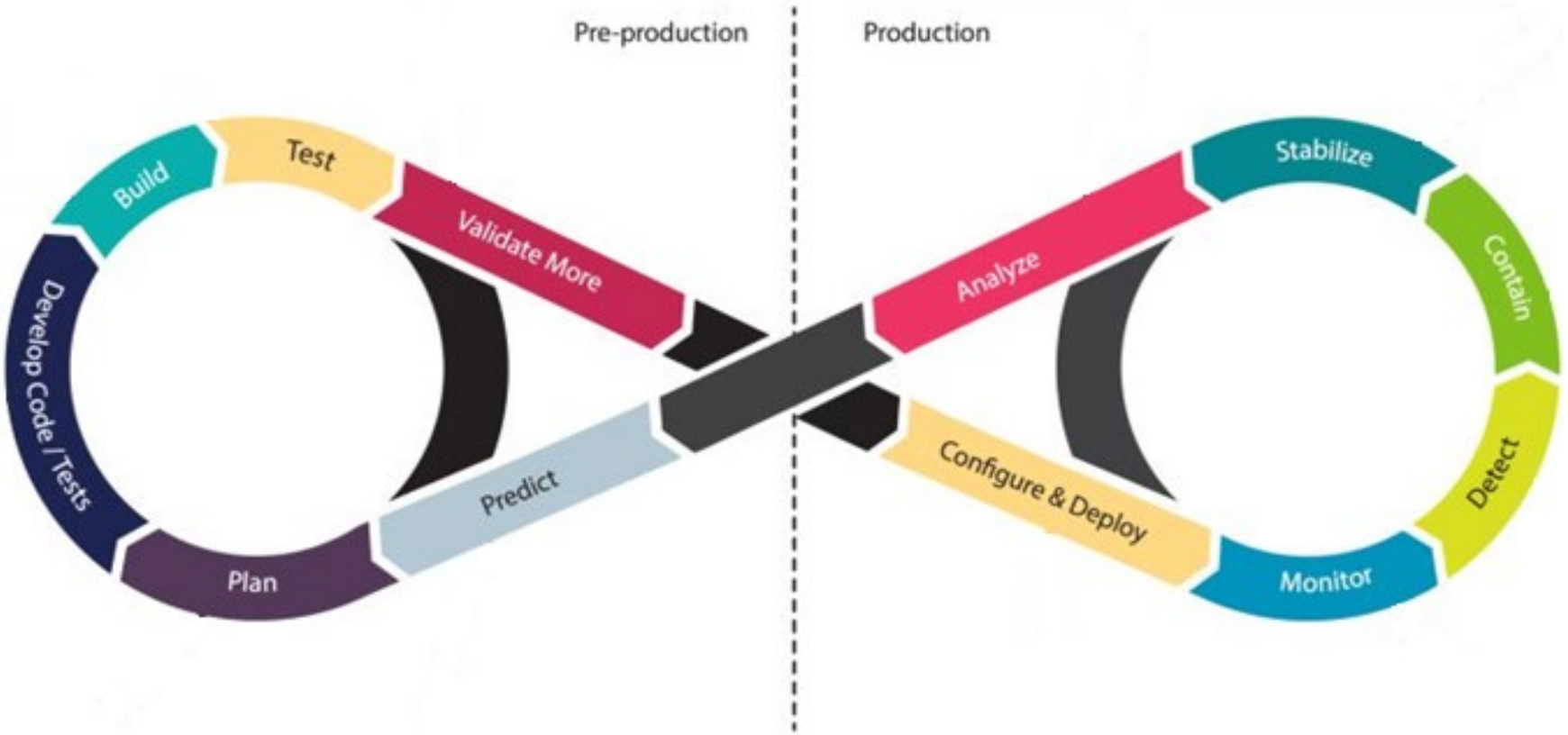
3,86 млн $
Средняя цена одной утечки данных[2]

67%

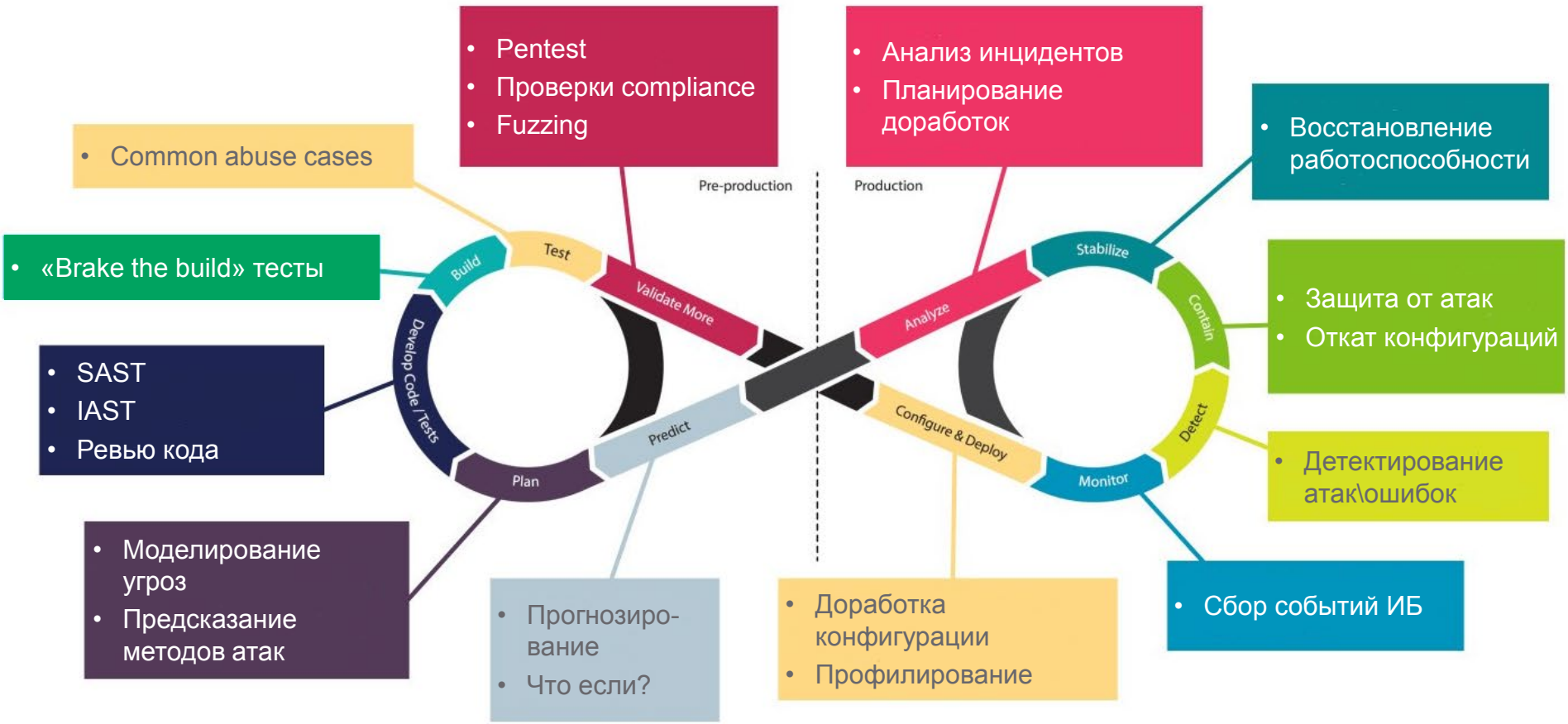
содержат критически опасные уязвимости[1]

[1] Positive Research 2018
[2] 2018 Cost of a Data Breach Study: Global Overview

КРОК


Pre-production
Production
Build
Test
Validate More
Develop Code / Tests
Plan
Predict
Analyze
Stabilize
Contain
Configure & Deploy
Detect
Monitor

KPOK


Pre-production
Production
Develop Code / Tests
Build
Test
Validate More
Predict
Plan
Analyze
Configure & Deploy
Stabilize
Contain
Detect
Monitor
• Common abuse cases
• «Brake the build» тесты
• SAST
• IAST
• Ревью кода
• Моделирование угроз
• Предсказание методов атак
• Pentest
• Проверки compliance
• Fuzzing
• Прогнозиро-вание
• Что если?
• Анализ инцидентов
• Планирование доработок
• Доработка конфигурации
• Профилирование
• Восстановление работоспособности
• Защита от атак
• Откат конфигураций
• Детектирование атак\ошибок
• Сбор событий ИБ

РАЗРАБОТКА И БЕЗОПАСНОСТЬ. ПРОБЛЕМЫ

Разрыв между «безопасником»
и разработчиками

Большое количество разработчиков
на одного аудитора

Высока цена ошибки/уязвимости

ОБЗОР ТЕХНОЛОГИЙ. КРАТКО

БЕЗОПАСНАЯ РАЗРАБОТКА SAST И DAST

КРОК

СИСТЕМЫ СТАТИЧЕСКОГО АНАЛИЗА

ТЕХНОЛОГИЯ SAST

ПРОБЛЕМЫ

- Рост объема кода
- Привлечение аутсорсеров для написания кода
- Разные языки
- Мало ИБ специалистов
- Использование небезопасных/ устаревших технологий

РЕШЕНИЕ

- Контроль кода на стадии написания
- Интеграция со средами разработки
- Стандартизированная и **автоматизированная** отчетность

СИСТЕМЫ ДИНАМИЧЕСКОГО АНАЛИЗА

ТЕХНОЛОГИЯ DAST

ПРОБЛЕМЫ

- Нет доступа к исходному коду приложения
- Нет возможности проверить найденную уязвимость
- Отсутствует автоматизированная отчетность об уязвимостях

РЕШЕНИЕ

- Набор проверок и правил (OWASP, WASC, CWE, CVE)
- Оптимизация времени, затрачиваемого на тесты
- Управление обнаруженными уязвимостями
- Продвинутая интеграция с конвейерами CI/CD

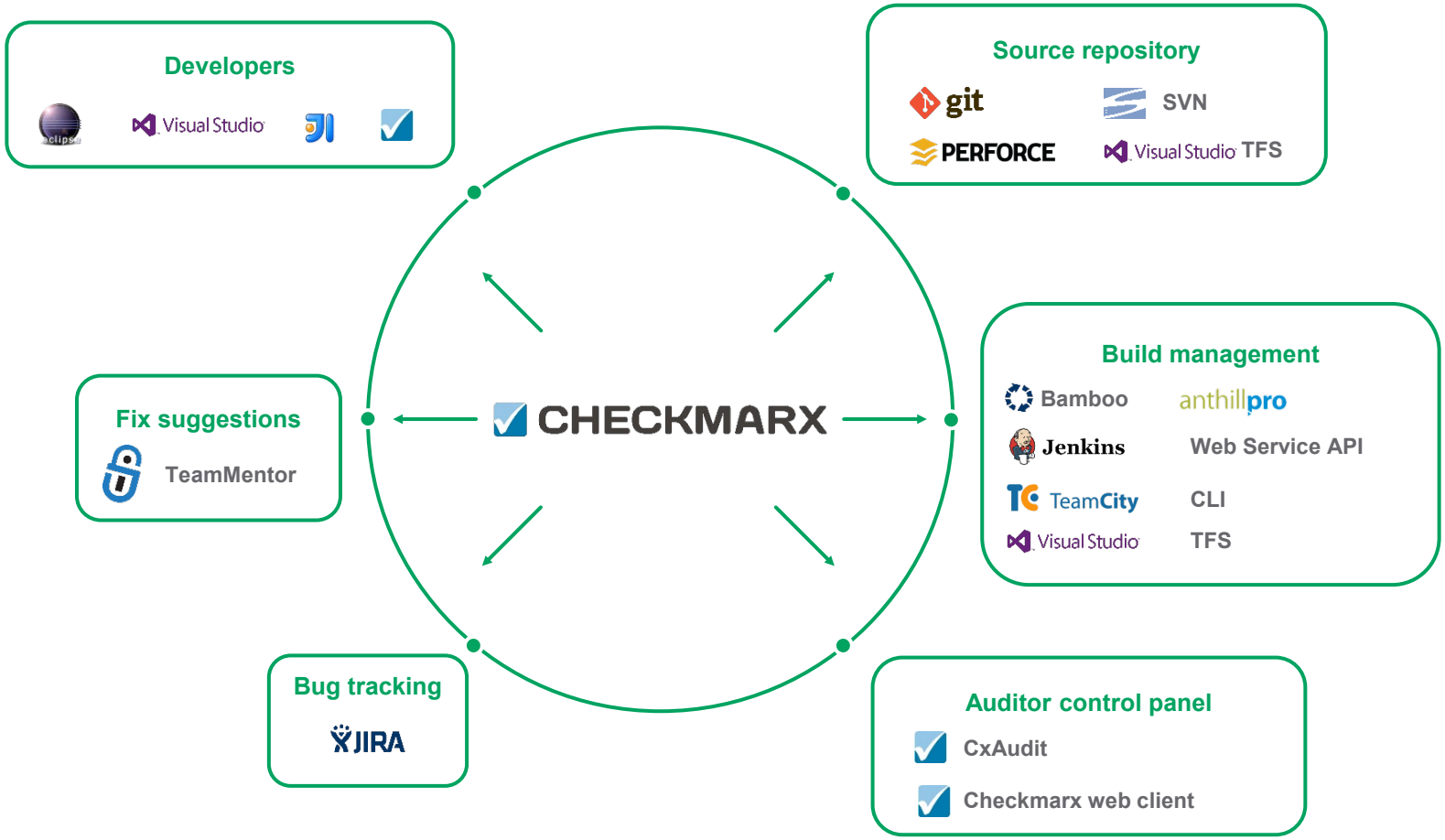
СИСТЕМЫ СТАТИСТИЧЕСКОГО АНАЛИЗА

ТЕХНОЛОГИЯ SAST

Source: Gartner (April 2019)

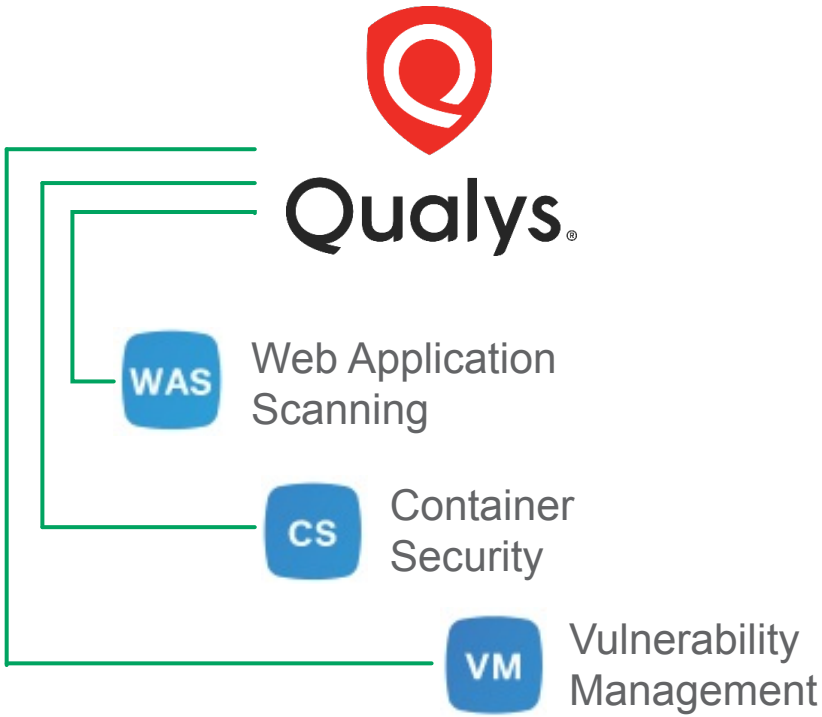
СИСТЕМЫ СТАТИЧЕСКОГО АНАЛИЗА

CHECKMARX



СИСТЕМЫ ДИНАМИЧЕСКОГО АНАЛИЗА

QUALYS

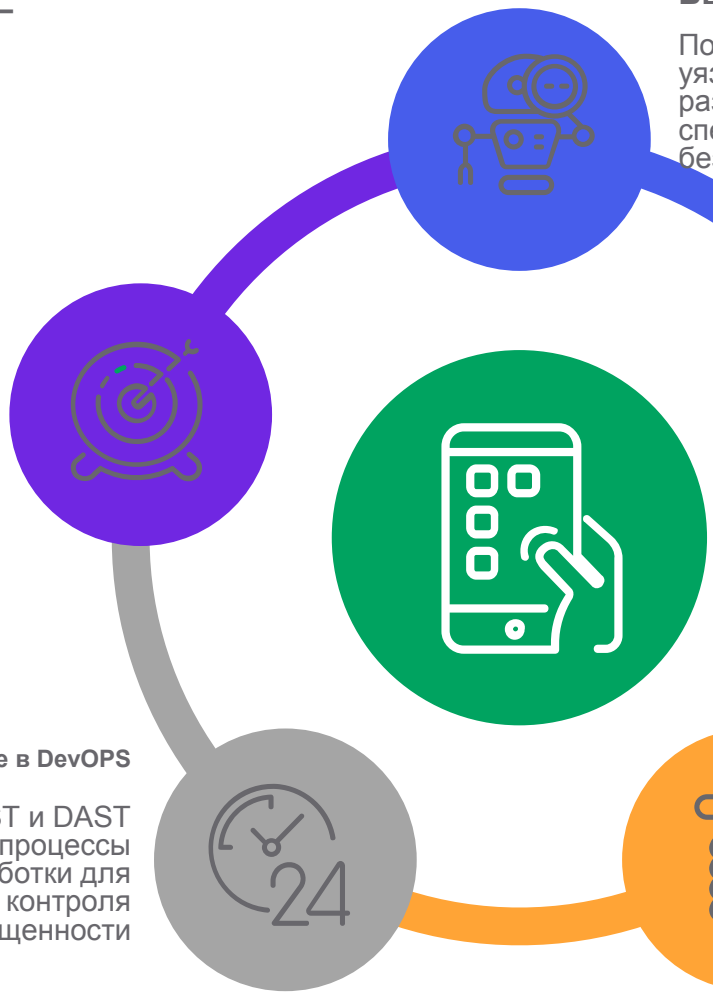


КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Эффективное сканирование веб-приложений, API и объектов контейнеризации
- Гибкие политики сканирования
- Управление уязвимостями
- Высокий уровень автоматизации и встраивание в CI/CD за счёт API

БЕЗОПАСНАЯ РАЗРАБОТКА

КРАТКИЙ ИТОГ



Выявление уязвимостей

Подробное описание уязвимостей для разработчиков и специалистов по безопасности

Автоматическое тестирование

Возможность тестирования выявленных уязвимостей приложений специализированными эксплойтами

Соответствие стандартам

Соответствие международным и отечественным стандартам в части безопасности приложений

Гибкое встраивание в DevOPS

Решения SAST и DAST встраиваются в процессы разработки для непрерывного контроля защищенности

Экономия

Экономия средств за счет нахождения и устранения ошибок и угроз на самом раннем этапе

БЕЗОПАСНАЯ ЭКСПЛУАТАЦИЯ WEB APPLICATION FIREWALL

КРОК

WEB APPLICATION FIREWALL

ОБЩЕЕ ОПИСАНИЕ

Решения класса Web Application Firewall (WAF) — средства фильтрации сетевого трафика, специально ориентированные на веб-приложения.

Предназначены для обнаружения и блокирования атак на веб-приложения и на их пользователей.

НОВОЕ ПОКОЛЕНИЕ WAF

ФУНКЦИОНАЛ

Защита от угроз
OWASP Top 10

Инспекция
SSL/TLS трафика

Автоматизация
работы WAF
при помощи API

Защита от кражи
учётных данных

Проактивная
защита от ботов

Защита
от DoS L7

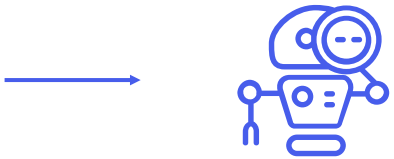
Автоматическое
обучение политик
защиты

ЗАКЛЮЧЕНИЕ

КРОК

БЕЗОПАСНАЯ РАЗРАБОТКА

Разрыв в знаниях



Общие методики
и практики тестирования.
Прозрачные показатели

Большое количество
разработчиков

Стандартизированная
и автоматизированная
отчетность

Высока цена ошибки

Выявляем ошибки
до момента релиза

КАК ВНЕДРЯЕМ

Подключение к облаку < 7 дней

On Premise < 3 месяцев

Помощь при выборе решения и возможность проведения пилота

Лучшая на рынке команда экспертов

Опыт внедрения в разных отраслях

КРОК

Проекты КРОК

01

КРУПНЫЙ РОССИЙСКИЙ БАНК

Использование SaaS-решения для защиты web-приложений в Облаке КРОК

02

МЕЖДУНАРОДНЫЙ БАНК

Повышение уровня защищенности информационных активов заказчика путем комплексного внедрения системы защиты электронной почты, защиты веб-приложений, динамического выявления, анализа и блокирования вредоносных файлов, на границе корпоративной сети

03

ТРАНСПОРТНАЯ КОМПАНИЯ

Внедрение Hybrid WAF решения для защиты критичных сервисов компании

04

КРУПНЫЙ РИТЕЙЛЕР

Внедрение OnPremise Web Application firewall в одном из крупнейших ритейлеров.
Защитой обеспечено более 70 Web-приложений

КРОК

СПАСИБО!

Александр Черныхов

Эксперт по информационной безопасности

AChernykhov@croc.ru

Андрей Крупнов

Директор по отраслевым решениям

AKrupnov@croc.ru