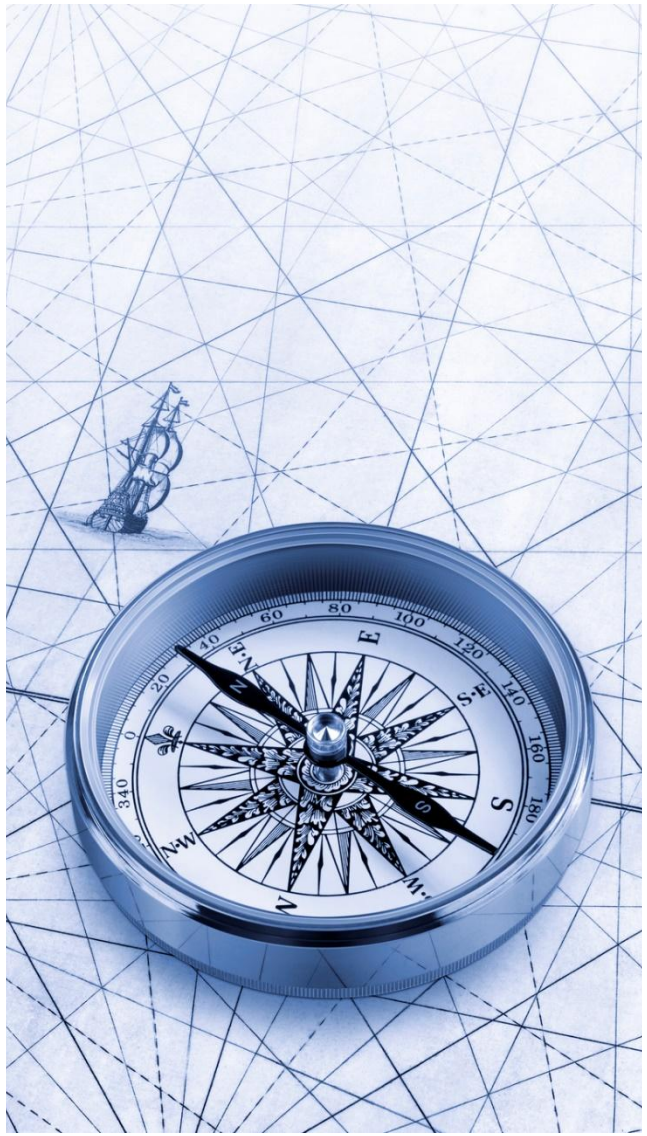
solidlab

Обеспечение безопасности критичных бизнес-приложений

Содержание презентации



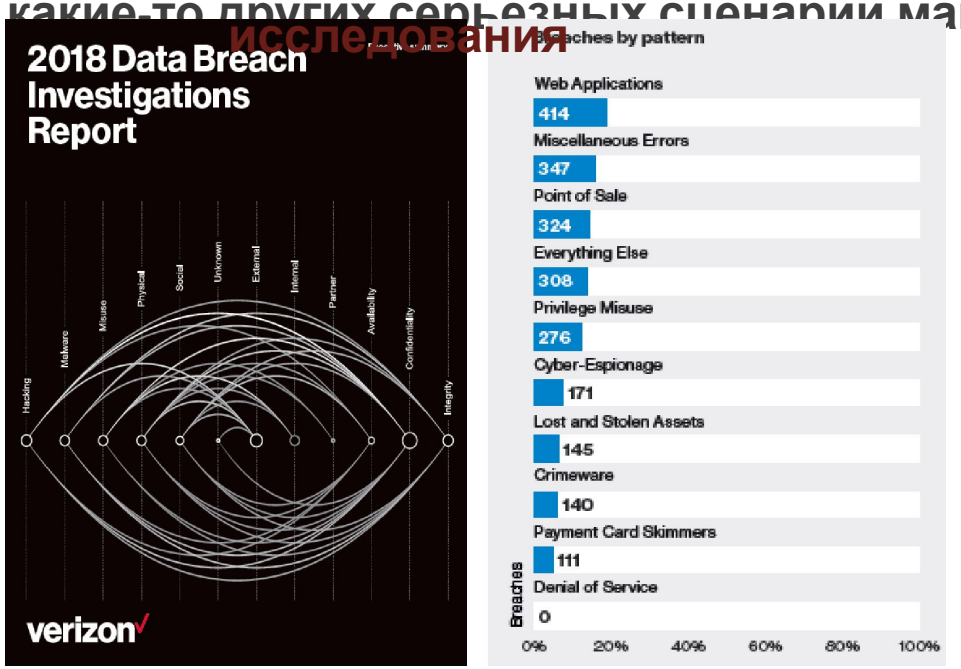
- О нашей компании
- Предпосылки для защиты приложения
- Наши решения по обеспечению безопасности приложений
- Подход к планированию и реализации проектов
- Вопросы - ответы

ПРЕДПОСЫЛКИ ДЛЯ ЗАЩИТЫ ПРИЛОЖЕНИЙ

Почему именно безопасность приложений?

- Веб приложения сейчас - это наиболее проблемная часть корпоративной ИТ-инфраструктуры.
- Злоумышленники либо используют непосредственно сами приложения либо используют их в качестве "точки входа" для того, чтобы добраться внутри организации ДО ЧЕГО УГОДНО.
- Если на периметре есть веб-приложения то вероятность проникновения внутрь сети, либо какие-то других серьезных сценарии максимальных этих очень высока

Внешние исследования



Собственный опыт


solidlab

СОГЛАСОВАНО
Генеральный директор
ООО «СолидЛаб»
Петухов А.А.
«XX» месяца 2017 г.

УТВЕРЖДАЮ
Директор по информационной безопасности Супер Банка
ФИО
«XX» месяца 2017 г.

Комплексный анализ защищенности информационной безопасности Супер Банка

Отчет о результатах анализа
XXXXXXXX.XX.XX.XX.XXX.X.OT

СОГЛАСОВАНО
Руководитель отдела управления проектами ООО «СолидЛаб»
Чернов А.В.
«XX» месяца 2017 г.

г. Москва,
2017 г.


3 РЕЗУЛЬТАТЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ВНЕШНЕГО ПЕРИМЕТРА КОРПОРАТИВНОЙ СЕТИ И ЕЕ КОМПОНЕНТОВ В МОДЕЛИ ВНЕШНЕГО НАРУШИТЕЛЯ - «ИНТЕРНЕТ ГОСТЬ» 10

3.1 Результаты анализа и найденные уязвимости сервиса: www.superbank.xx 10

3.1.1 SL-BANK-REDTEAM-01: доступность сервиса в обход сети очистки трафика «QRator». 10
3.1.2 SL-BANK-REDTEAM-02: подробные сообщения об ошибках 12
3.1.3 SL-BANK-REDTEAM-03: возможность внедрения операторов SQL 13
3.1.4 SL-BANK-REDTEAM-04: хранение учетных данных без хеширования 14
3.1.5 SL-BANK-REDTEAM-05: возможность обхода URL-фильтрации при доступе к административному интерфейсу 15
3.1.6 SL-BANK-REDTEAM-06: возможность загрузки cfm-файлов через административный интерфейс 18
3.1.7 Недостаточный мониторинг безопасности серверов официального сайта. 19

3.2 Развитие атаки внутрь корпоративной сети после получения возможности выполнения кода на официальном сайте 19

Подпись и дата | Инв. № дубл. | Взам. инв. № | Инв. № подл.
Изм. Лист № докум. Подп. Дата
Разраб.
Пров.
Н. контр.
Утв.
XXXXXXXX.XX.XX.XX.XXX.X.OT
Отчет о комплексном анализе защищенности ИБ
Лит. Лист Листов
1 82
solidlab

Современные тренды в области безопасности приложений

Активная автоматизация сложных бизнес-процессов

Значительное влияние на бизнес, высокий потенциальный ущерб

Уникальные характеристики ключевых бизнес-процессов

Сокращение времени для выпуска продукта (Time to production)

Усложнение разрабатываемых приложений, большой объем задач по разработке

Высокий уровень кастомизации приложений

Использование заимствованных компонентов и повторное использование собственных

Активный

Увеличение технологических возможностей атак

Развитие киберпреступности

Направленные атаки, 0-day и 1-day атаки

Отставание средств защиты от технологий разработки

Недостаток ресурсов и компетенций

Проблемы «классического» подхода к обеспечению безопасности

Требуемая бизнесом скорость публикации приложений делает существующие практики безопасности неэффективными из-за длительного времени экспозиции уязвимостей

Имеющиеся методы динамического анализа и мониторинга не позволяют обеспечить полноту выявления уязвимостей

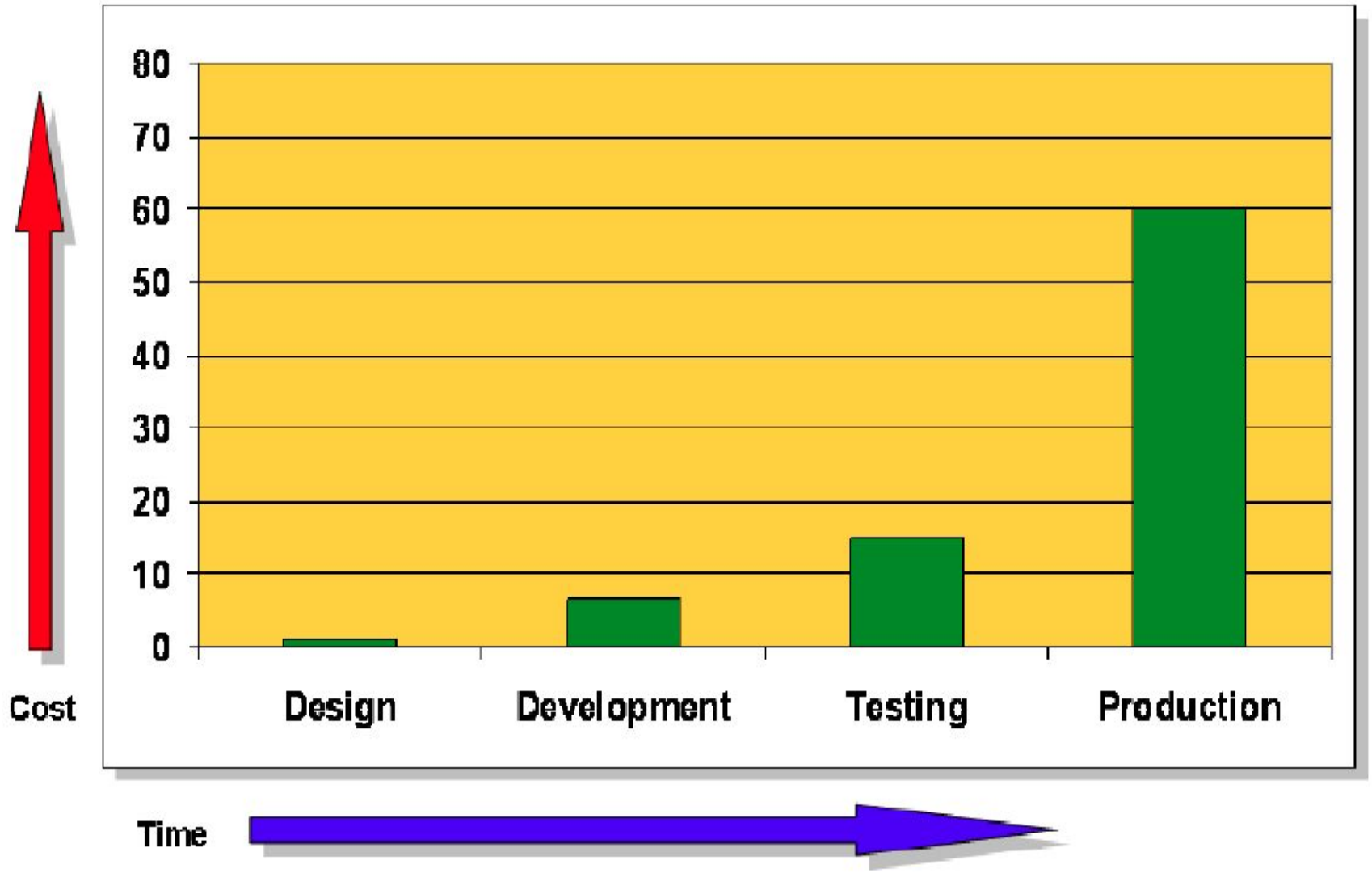
Не обеспечивается «сходимость» процесса – уязвимостей не становится меньше со временем.

Анализ защищенности выполняется на этапе приемки, или, что еще хуже – на этапе эксплуатации, когда исправлять приложение очень дорого или невозможно

Любое изменение системы требует перенастройки средств безопасности, по-хорошему, нового анализа защищенности

Либо большое количество ложных срабатываний приводит к тому, что мониторинг работает неэффективно

Вопрос финансов: чем раньше – тем лучше.



О НАШЕЙ КОМПАНИИ

О нас

- **Более 150 успешно завершенных проектов**
- Основу нашей команды составляют выпускники, аспиранты и исследователи факультета ВМК Московского Государственного университета.
- Наши эксперты выступают на ведущих конференциях, посвященных практической безопасности.
- Наши специалисты активно участвуют в CTF-соревнованиях в составе команды «Bushwhackers». Участники команды неоднократно побеждали в специализированных хакерских конкурсах.
- Наши эксперты включены в залы славы по итогам участия в bug-bounty программах на сайтах крупных ИТ-компаний, имеют благодарности от разработчиков известных платформ и продуктов.
- Компания SolidLab успешно работает на российском и зарубежном рынке информационной безопасности.
- Среди наших клиентов – крупнейшие организации из различных секторов экономики: интернет-компании, финансовый сектор, телеком, промышленность, энергетика

Наши решения по обеспечению безопасности приложений

• Как выявить текущие недостатки защиты и устранить их в кратчайший срок? • Как обеспечить безопасность для приложений с «классическим» подходом к разработке и «медленным» релизным циклом?	**РЕШЕНИЯ ПО АНАЛИЗУ ЗАЩИЩЕННОСТИ**
• Как снизить количество недостатков и времени их экспозиции в перспективе? • Как организовать безопасность приложений с современным подходом к разработке и активным релизным циклом?	**ПОСТРОЕНИЕ ПРОЦЕССОВ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРИЛОЖЕНИЙ**
• Что делать с недостатками конфигурирования приложения и инфраструктуры его доставки при публикации? • Как быть с недостатками эксплуатации (управление доступом, мониторинг и т.п.)? • Как обеспечить безопасность среды разработки?	**ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ DEVOPS**
	МОНИТОРИНГ СОБЫТИЙ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ
	БЕЗОПАСНОСТЬ СРЕДЫ РАЗРАБОТКИ

АНАЛИЗ ЗАЩИЩЕННОСТИ

Внешние и внутренние бизнес-приложения

- Инфраструктура доставки приложений
- Мобильные приложения
- Пользовательская инфраструктура
- Процессы и персонал
- Стандартные сетевые сервисы
- Беспроводные сети
- Технологические системы и сети
- Сервисы удаленного доступа

Технологии

- код приложений (собственный, фреймворк, сторонние библиотеки)
- прикладные компоненты: сервер приложения, сервисы очередей, кеша (memcached) и т.п.
- системные компоненты: ОС узла, системные демоны
- сторонние службы: СУБД, AD, backend-системы
- сетевые компоненты: доступ к приложению, связь рабочих станций
- системы защиты

Процессы

- разработка или заказ/принятие кода
- управление изменениями
- развертывание (интеграция) и настройка
- обновления ПО (собственного и стандартного)
- управление учетными записями и привилегиями
- администрирование всего вокруг (сети, СУБД, ОС, прикладных служб)
- мониторинг срабатываний и настройка средств защиты

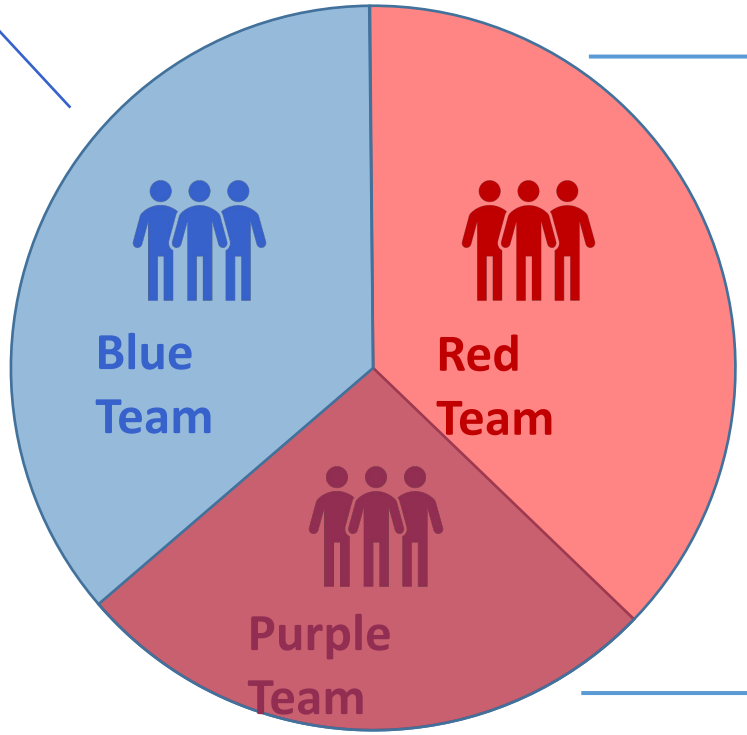
Несанкционированный доступ к критичной информации, ее модификация, нарушение целостности или уничтожение

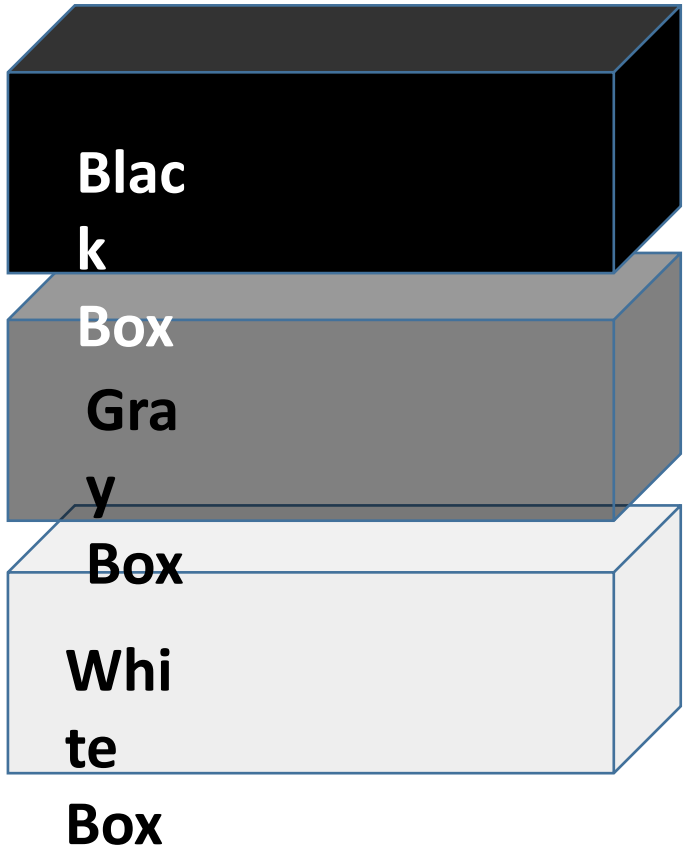
Выполнение несанкционированных действий в информационных системах (например, перевод денежных средств и т.п.)

Нарушение доступности или снижение производительности информационных сервисов

Нарушение требований законодательства, иных внешних или внутренних требований

- Интернет-пользователь без прав во внешних приложениях
- рядовой пользователь внешних приложений
- порождаемые использованием мобильных приложений
  - человек посередине в Wifi-сети, вредоносное приложение, похищенное устройство, доступ к SIM-карте
- внутренний рядовой пользователь корпоративной сети
- удаленный пользователь корпоративной сети, подключающийся через VPN
- гость офиса с доступом к ethernet-розетке
- гость офиса с доступом к гостевой беспроводной сети
- гость офиса в зоне действий корпоративной wifi-сети



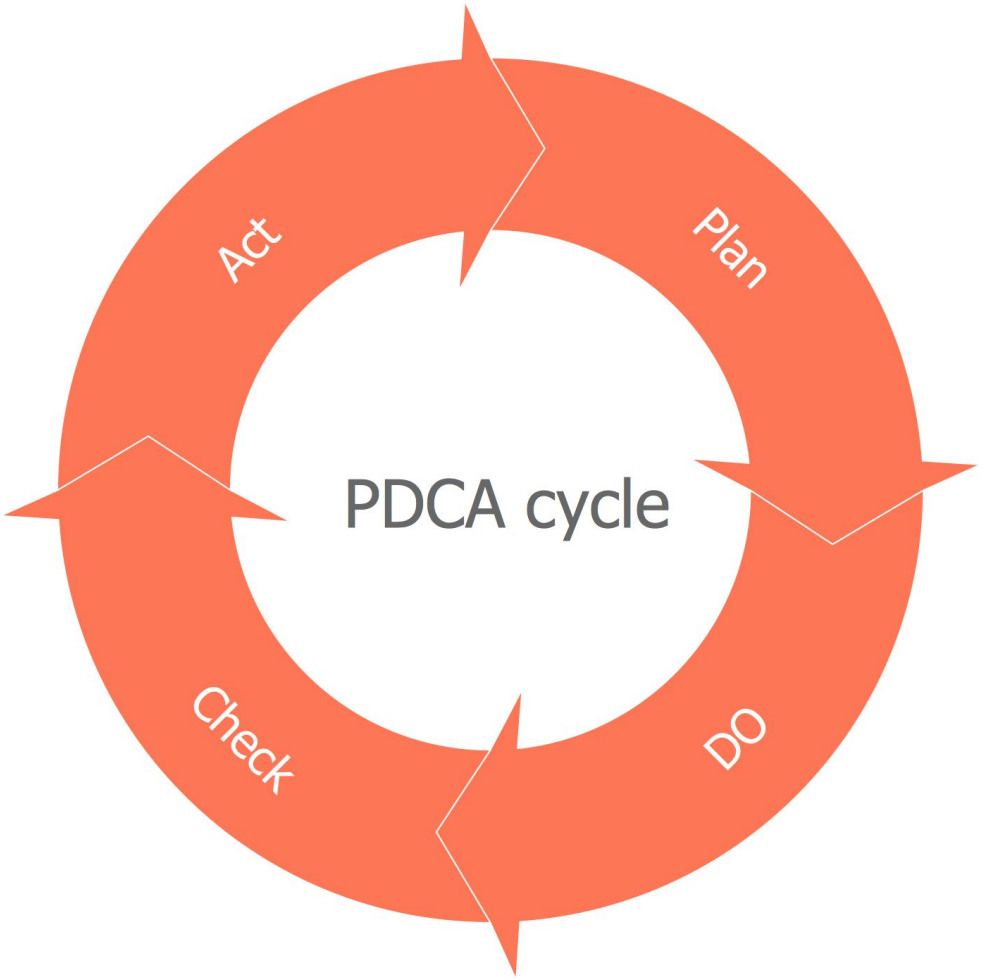


Тестирование на проникновение

Полный анализ защищенности

- Все легально
- Работаем в максимальном контакте с клиентом, чтобы исключить влияние проводимых работ на критичные бизнес-процессы
- Преимущественно ручные методы работы, специальный инструментарий (в т.ч. собственной разработки)
- Лучшие практики: ISO, NIST, Certified Ethical Hacker, OSSTMM Web Application Methodology, OWASP Testing Guide
- Анализ исходного кода приложений, анализ конфигураций компонентов ИТ-инфраструктуры (в режиме «белого ящика»), бинарный анализ
- Специальное оборудование для тестирования беспроводных сетей
- Реальные сценарии социальной инженерии: фишинговые ссылки, эксплоиты, контакты с сотрудниками организации

- **Резюме для руководства**
  - какие процессы не работают, какие работают
  - какие негативные сценарии могут случиться в текущем состоянии
- **Цель проведения работ, область проведения, методика**
- **Список найденных недостатков**
  - как воспроизвести (воспроизводимость – архиважно!)
  - анализ критичности: какие последствия могут наступить
  - рекомендации по исправлению
- **Список подтвержденных защитных мер (что хорошо)**
- **Общие выводы и предлагаемый план**
  - краткосрочные меры, среднесрочные, долгосрочные.
  - последующие шаги с SolidLab: повторная проверка, помощь с тонкой настройкой средств защиты, более детальный анализ какой-то области или подсистемы
- **Приложения с техническими данными**
  - журналы проверок, исходные коды эксплойтов, снимки экранов, протоколы социальных воздействий, примеры скомпрометированных данных и т.п.



ПОСТРОЕНИЕ ПРОЦЕССОВ БЕЗОПАСНОЙ РАЗРАБОТКИ

Основные характеристики проекта

Проект

500 000 строк

Жизненный цикл

- Внешняя разработка
- Активный релизный цикл
- Внутренняя разработка
- Традиционный релизный цикл

Agile. Релиз – один раз в две недели.

Команда

15 разработчиков, Secutiy TL отсутствует

Java, Фреймворк Java Beans

Eclipse, Git, Jenkins, Jira

Статический анализ MF Forify При приемке – Whitebox анализ

Технологии

Java, JS, php, python, Groovy, Android, Apple, HTML5, Windows Mobile, C++, ASP.net, VB.NET, Visual Basic 6.0, PL/SQL, perl, Ruby, C#.net, Apex, Swift, Scala

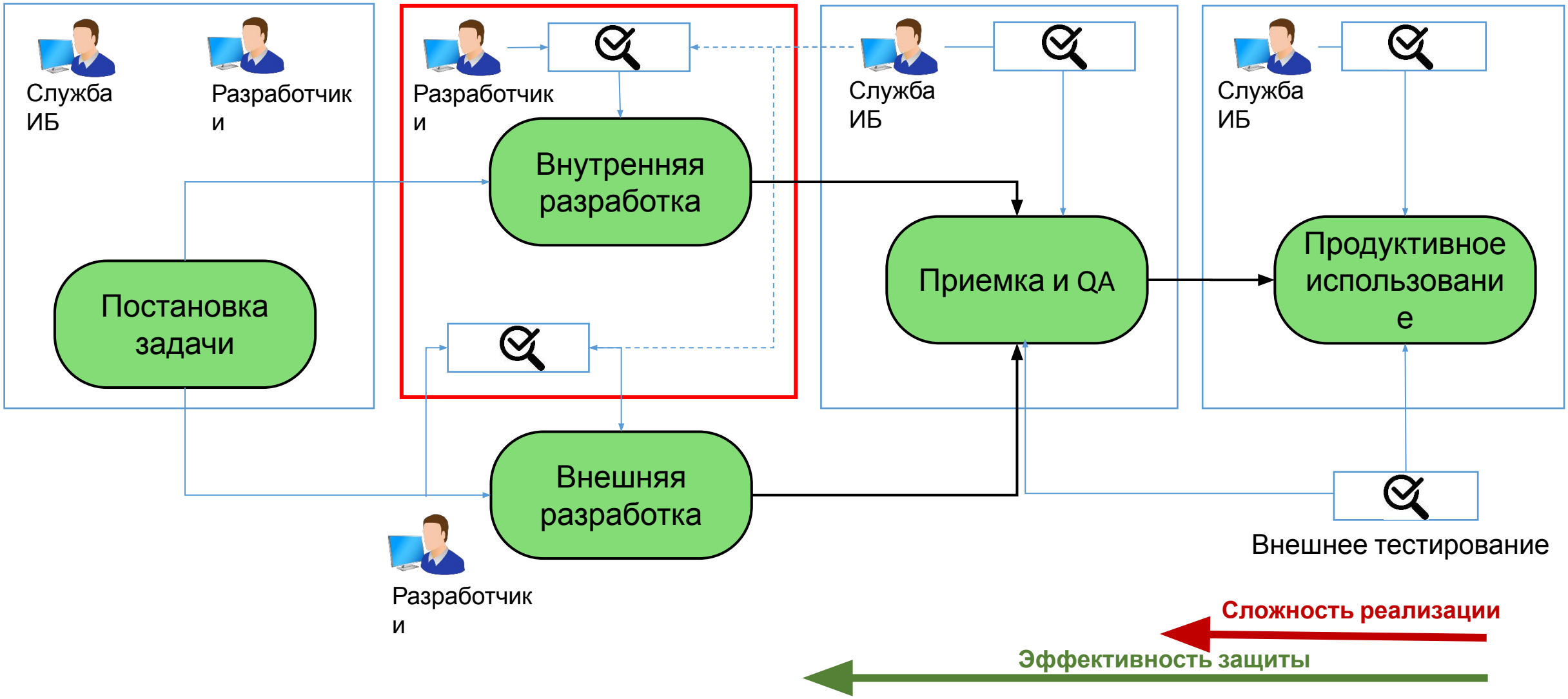
Инструменты

- Web Client
- Eclipse plugin
- Visual Studio plugin
- Intellij plugin
- TFS (Team Foundation Server)
- SVN (Subversion)
- GIT
- Perforce
- JIRA
- Bamboo
- Jenkins
- WS API
- CLI
- Sonar

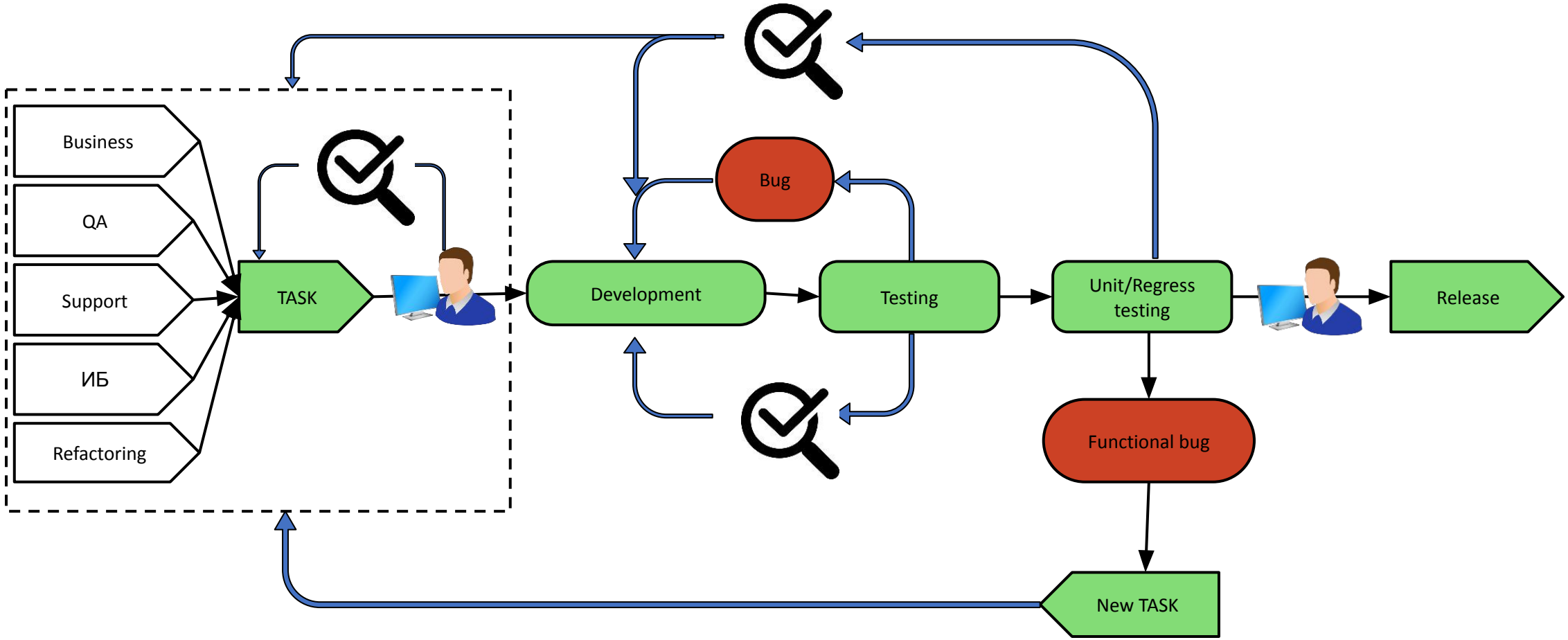
Выбранный подход к ИБ

- Безопасность – отдельный этап
- Автоматический анализ
- Безопасность – часть процесса
- Ручной анализ

Жизненного цикла проекта (pipeline)



Жизненный цикл проекта. Этап разработки



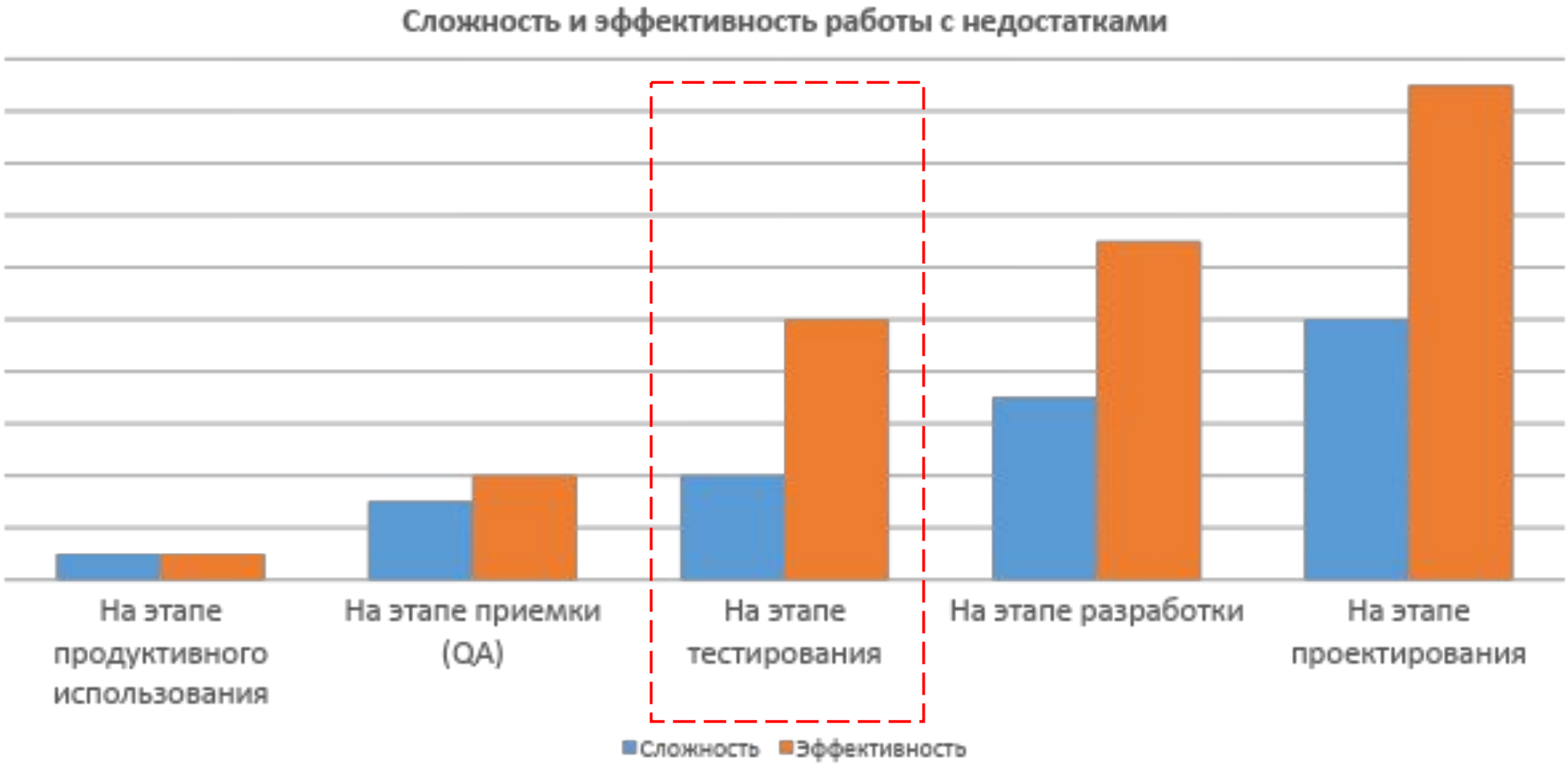
Автоматизированный анализ

Ручной анализ

Внешний анализ

Этапы цикла разработки

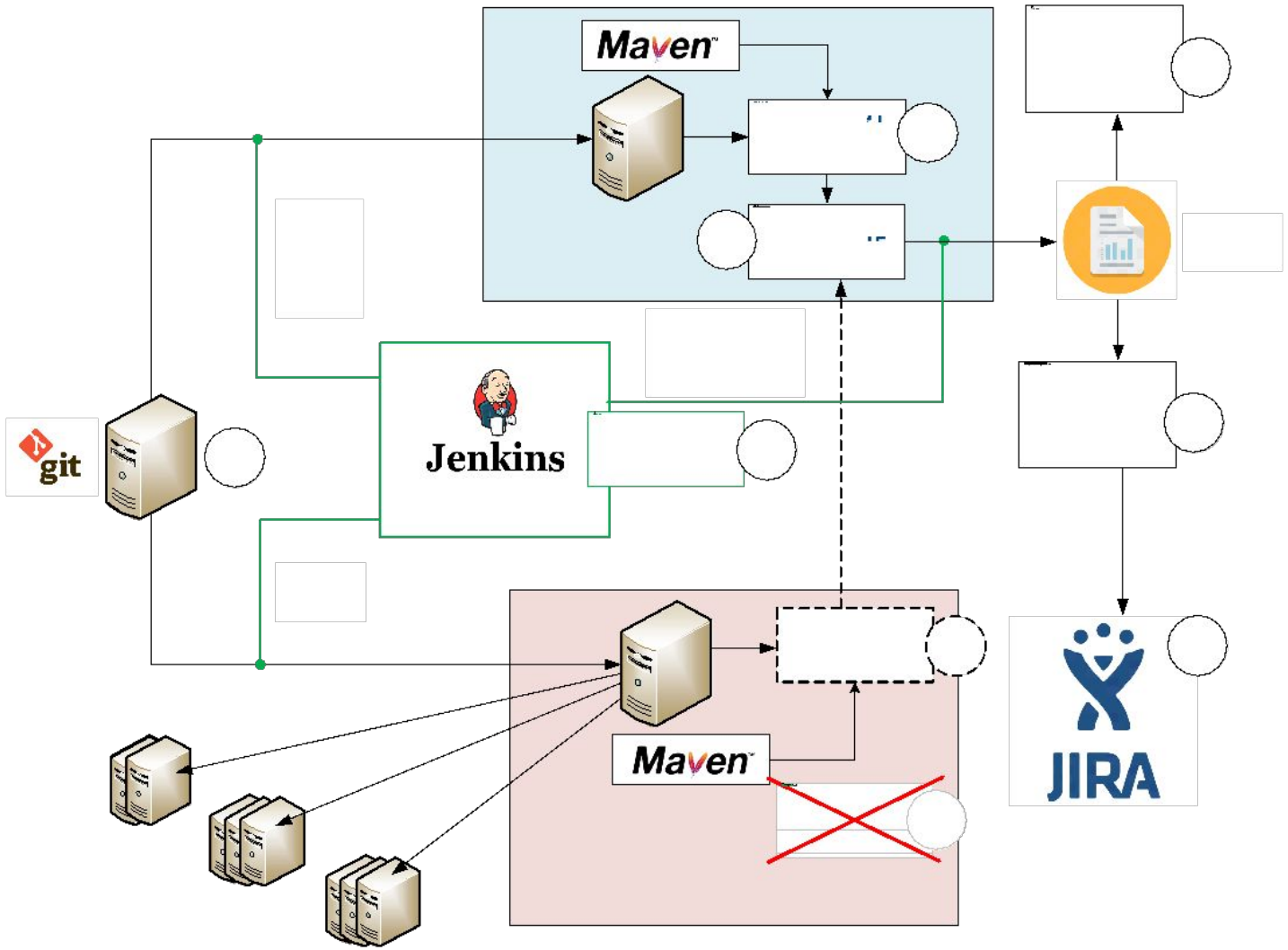
Выбор подхода к обеспечению ИБ



Решения для построения процесса безопасной разработки

- Системы статического анализа
- Системы динамического анализа
- Средства анализа внешних компонентов
- Межсетевые экраны уровня приложений
- Ручной анализ защищенности приложений
- Bug-Bounty программа
- Обучение практикам и инструментам безопасной разработки

Система статического анализа (пример технической реализации)



Ключевые вопросы

- Применимость средства, поддержка используемых фреймворков и практик разработки
- Тонкая настройка правил для подавления ложных срабатываний и обеспечения полноты анализа.
- Интеграция с текущим процессом разработки: в каком месте, каким способом и т.п.
- Обучение специалистов Заказчика и активное вовлечение разработчиков в процесс

Обучение специалистов

Руководители команд разработки (Team

Разрабо

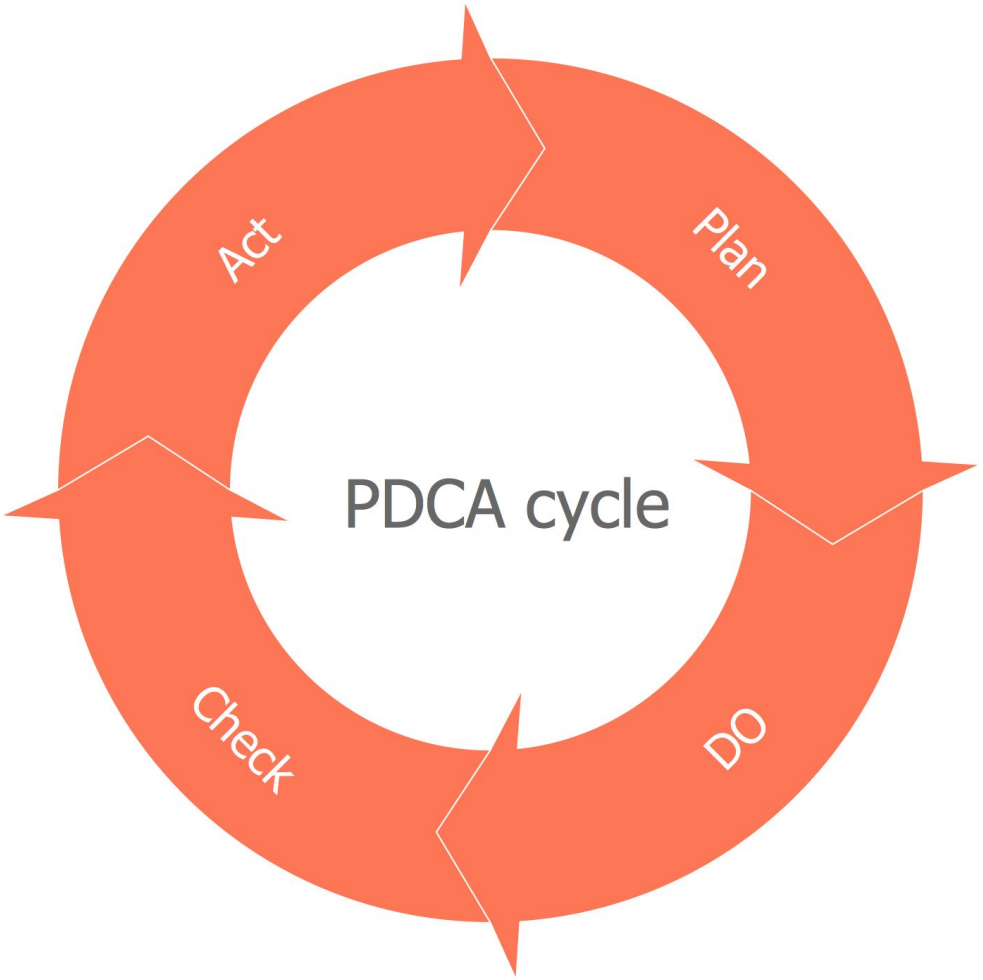
Инженеры разработки (DevOps)

Специалист ы ИБ

Модуль 1. Типовые уязвимости веб-приложений - 6ч	Введение
	Инъекции и санитизация запросов во внешние подсистемы
	Валидация сложных форматов
Модуль 2. Аутентификация и авторизация - 8 ч	Аутентификация
	Авторизация
Модуль 3. Модуль 3. Обзор OWASP Top 10 - 3 х	Краткая характеристика угроз из OWASP Top 10
Модуль 4. Использование средства статического анализа - 8 часов	Обзор принципов работы стат. анализаторов и их ограничений
	Использование средства статического для выявления недостатков
	Настройка средства статического анализа

Сопровождение проектов

- ✔ Техническая поддержка иструментов безопасной разработки
- ✔ Взаимодействие с вендором
- ✔ Анализ исходного кода и выявление недостатков
- ✔ Подтверждение эксплуатабельности, оценка рисков
- ✔ Экспертные консультации по вопросам безопасной разработки

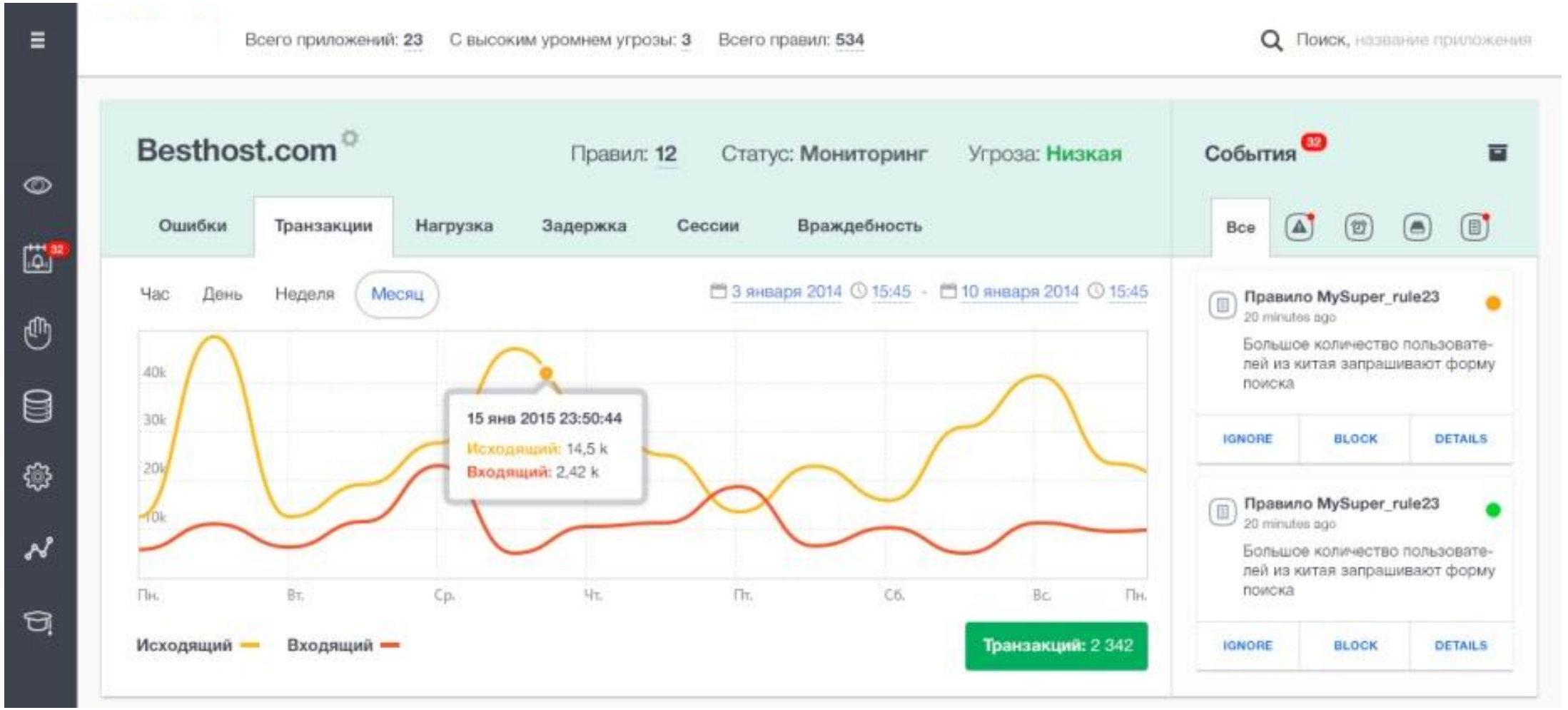


ПРЕДОТВРАЩЕНИЕ НЕДОСТАТКОВ КОНФИГУРАЦИИ И ЭКСПЛУАТАЦИИ

Обеспечение безопасности DevOps

Мониторинг угроз и реагирование на инциденты

Web Application Firewall – Интеллектуальный сетевой экран уровня приложений



Профессиональные сервисы

Сервисы оказываются высококвалифицированными российскими специалистами, имеющими богатый опыт в области противодействия интернет-угрозам

- Анализ уязвимостей WEB-ресурсов и оценка связанных с ними рисков информационной безопасности.
- Пилотное тестирование предлагаемого решения для оценки его потенциальной эффективности.
- Техническое проектирование и внедрение системы SolidWall в инфраструктуру Заказчика.
- **Тонкая настройка системы для защиты конкретных WEB-приложений**.
- **Мониторинг угроз**
- Разработка процесса реагирования на инциденты информационной безопасности. Поддержка клиента при расследовании инцидентов ИБ.
- Обучение персонала заказчика навыкам работы с системой, а также основам противодействия угрозам в сети Интернет.
- Техническая и консультационная поддержка.
- Адаптация WAF под изменения приложений клиента.
- Подключение дополнительных приложений.
- Изменение функциональности WAF по запросу клиента (формы отчетности, изменение сценариев работы пользовательским интерфейсом).
- Интеграция со сторонними средствами (SIEM, тикет-системы, СМС-информирование и т.п.).

BugBounty программа

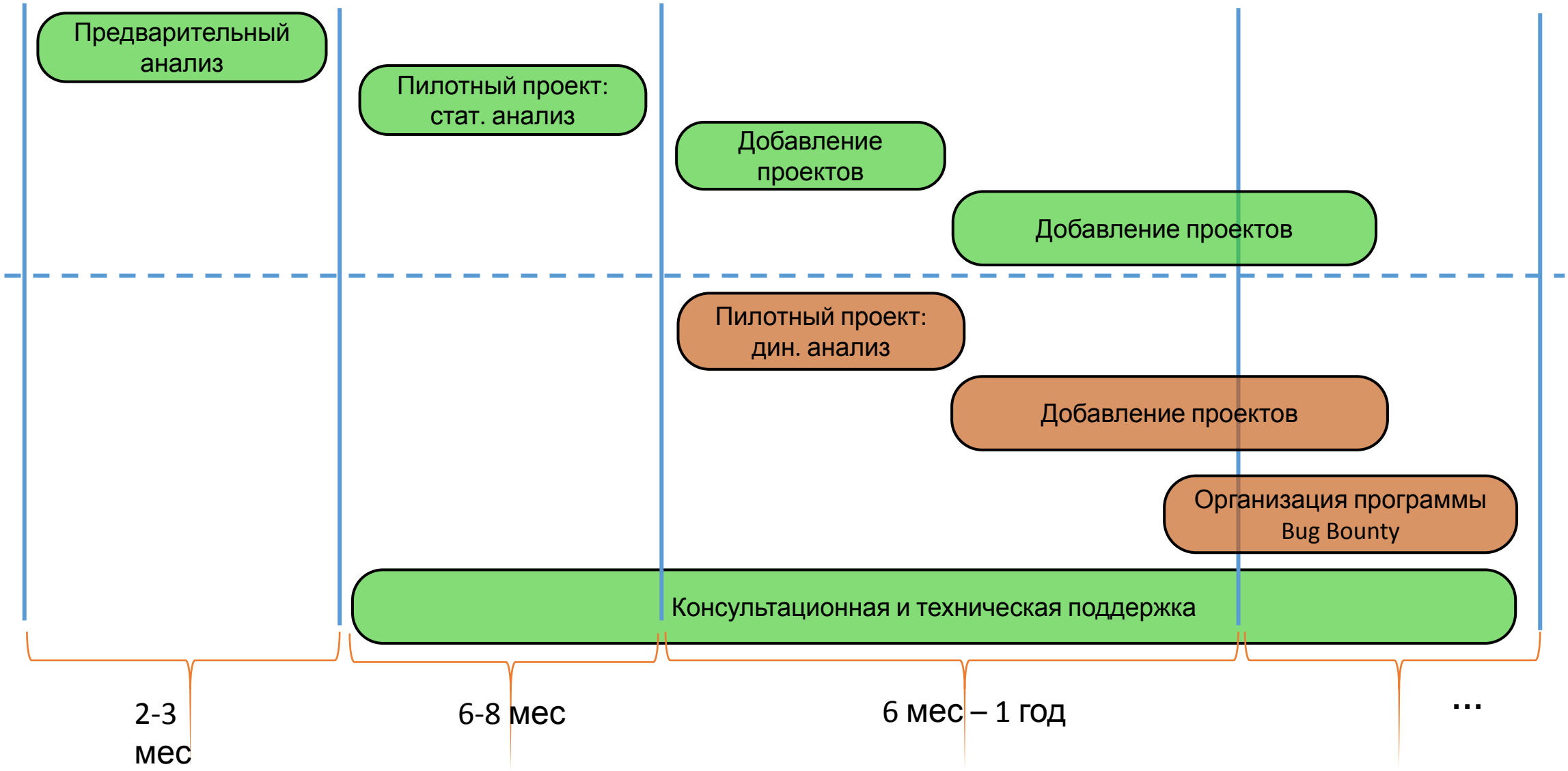
Ключевые вопросы

- Принятие решения о старте программы
- Условия и формат программы
- Организация процесса: отсев мусора и дубликатов, проверка эксплуатабельности, принятие решения о выплате, исправление уязвимостей, обратная связь на процесс разработки
- Обучение и поддержка специалистов Заказчика

Обеспечение безопасности среды разработки

РЕАЛИЗАЦИЯ ПРОЕКТОВ

Внедрение процессов безопасной разработки



Ваши вопросы?

Вячеслав Железняков
Директор по развитию