Безопасность — сочетание организационных и технических мер

- Автоматика не решит проблему полностью, человеческий контроль также важен
- Если специалиста по безопасности нет, то самый простой способ — делегировать это в QA
- Security внедряют не от «хорошей жизни», а из необходимости
- Нужно выдерживать баланс между скоростью разработки и безопасностью

SimbirSoft

Неочевидные угрозы безопасности

Человек, который пишет код

Самая неочевидная угроза безопасности кода.

Выстраивание функционала вокруг проблемы в безопасности

Например, произвольное исполнение SQL-запроса: если пользователь авторизован, то может получить результат любого запроса, даже не своего.

Сжатые сроки

Порождают временные решения, которые не отвечают требованиям безопасности. Например, не используется внешнее хранилище, пароль хранится в коде.

Кадровый голод

Приводит к тому, что на должность приглашаются специалисты с недостаточным уровнем компетенций. В частности, в решении и предупреждении проблем безопасности.

Неочевидные угрозы безопасности

Варианты решения

Моделировать возможные угрозы и ставить себя на место злоумышленника.

Следить за качеством кода — это поможет сильно сократить количество багов безопасности. Одна из мер для создания качественного кода — регулярное проведение код-ревью.

Подключить к работе специалиста по безопасности. Зачастую разработчик не обладает необходимым образом мышления и компетенциями для предупреждения угроз безопасности и оперативного устранения проблемы.

Инструменты для обеспечения безопасности

старт → 1 → 2 → 3 → 4 → 5 → 6 → релиз

Архитектурное ревью

— Принимать меры по безопасности продукта нужно на старте разработки. Это позволит предупредить дальнейшие затраты на решение проблем.

— Часто требования по безопасности приходят сразу от клиента. Например, соответствие стандарту безопасности данных платежных приложений.

Набор чек-листов для команд

Проверка библиотек сканером безопасности OWASP dependency check

Проведение SAST — позволяет находить уязвимости в исходном коде во время разработки. Получение моментальной обратной связи по безопасности, например, с помощью Snyk

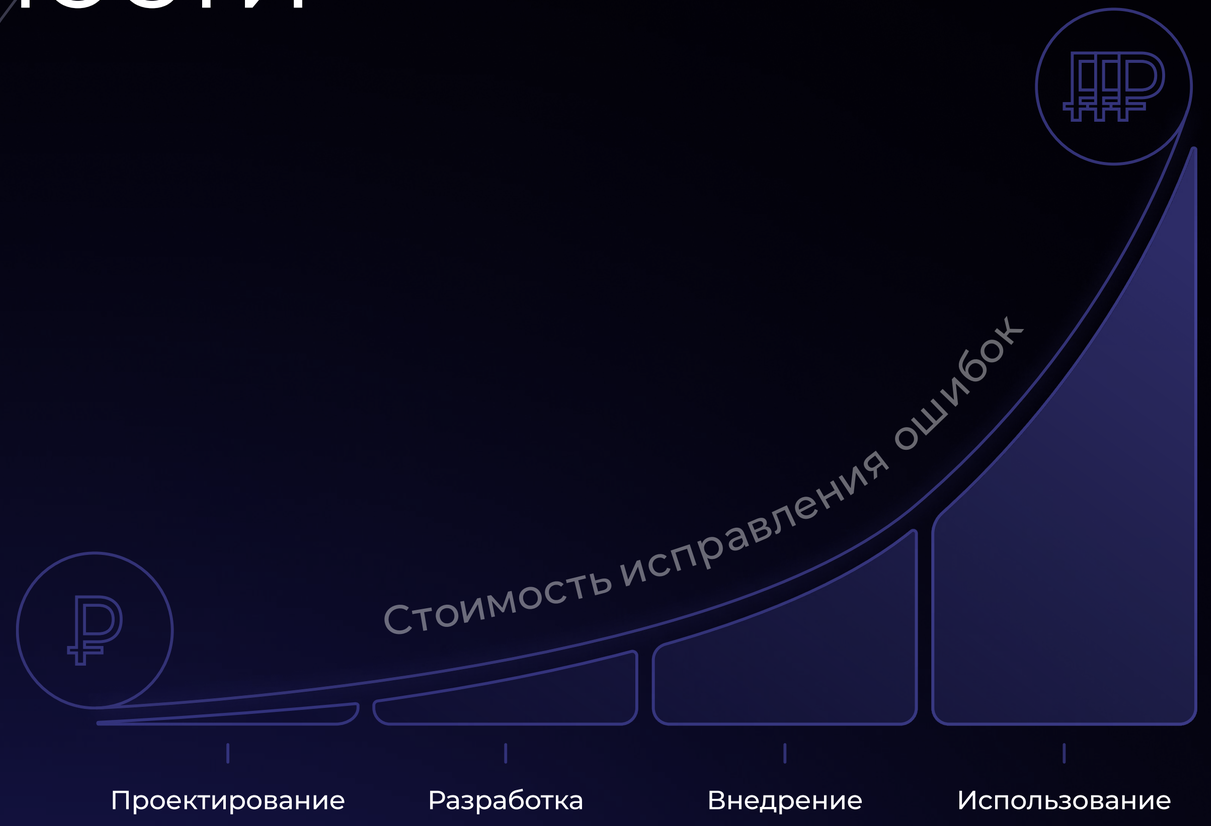
Сканирование во время рабочего процесса с последующим мониторингом. Например, с помощью DefectDojo

Проверка с помощью DAST на финальном этапе разработки приложения

SimbirSoft

Вложения во внедрение средств анализа безопасности

Вкладывать в анализ безопасности также важно, как и в тестирование.
Стоимость исправления ошибки на этапе ревью во много раз ниже, чем при обнаружении на стороне клиента.



SimbirSoft

Реакция команд на security checks

Самая распространенная реакция — негатив:
«Безопасник не разработчик, чему он нас научит?»

Что с этим делать?

Вскрыть реальную уязвимость кода (Pain-Driven Security). Например, с помощью инструмента BurpSuite. «Security внедряют не от «хорошей жизни», а из необходимости».

Объяснить сотрудникам, что мы внедряем не средство контроля, а помощь в виде инструмента.

Обучать специалистов и выделять ошибки постепенно. На первых этапах нужно налаживать отработку и устранение ошибок без остановки рабочего процесса. Затем — можно прерывать пайплайны.

Передать на penetration test на финальной стадии работы над продуктом, чтобы проверить его на пропущенные уязвимости.

Постепенно на место негатива приходит понимание, зачем это нужно и почему важно.

Отказ от обновления версий библиотек

> Сторонние библиотеки содержат вредоносное ПО, и количество таких случаев растет

Но это не повод отказываться от обновлений

Проблемы необновленных библиотек:

1 / 3

Можно не получить обновление с фиксом более страшной проблемы

2 / 3

Торможение развития продукта

3 / 3

Проблемы с аудитом и поддержкой в будущем

Как решать проблему обновлений библиотек

Создать «буферную зону» — загружать библиотеки в собственное хранилище, проверять и только затем принимать решение об использовании.

— Обновления получаем не в real-time, но прикрыты от уязвимостей.
— Если библиотека давно не обновлялась, то можно не пройти аудит. В этом случае локальное хранилище также поможет.

Как только выйдет проверенная версия, можно выполнить обновление. Если этого не произойдет, рассмотреть аналоги.

Проводить регулярный мониторинг и аудит. Нужно внимательно следить за списками изменений (release notes), некоторые могут быть не нужны.

«Безопасник нужен, чтобы однажды не проснуться бедными»

SimbirSoft